Tulsa Journal of Comparative and International Law

Volume 9 | Issue 2 Article 2

3-1-2002

Right to Privacy in Personal Data: The EU Prods the U.S. and Controversy Continues, The

Marsha Cope Huie

Stephen F. Laribee

Stephen D. Hogan

THE RIGHT TO PRIVACY IN PERSONAL DATA: THE EU PRODS THE U.S. AND CONTROVERSY CONTINUES

Marsha Cope Huie[†] *Stephen F. Laribee*[††] *& Stephen D. Hogan*[†††]

> "We are writing to reinforce our concerns over the proposed standard contract clauses as described in the [U.S.] Treasury-Commerce joint letter on Feb. 16, 2001.... The proposed standard clauses are not a workable model. They impose unduly burdensome requirements that are incompatible with real world operations."
>
> – Letter to EU Commission simultaneously released to the Press from the U.S. Dept. of Commerce, March 23, 2001.[1]

[†] B.S., M.A., University of Tennessee, Knoxville, Tennessee; J.D., University of Memphis, Memphis, Tennessee; LL.M., University of Cambridge, United Kingdom; Visiting Professor, University of Tulsa College of Law, Tulsa, Oklahoma.

[††] D.B.A., C.P.A.; Eastern Illinois University, Charleston, Illinois.

[†††] Ph.D.; John Massey Chairholder in Finance, Southeastern Oklahoma State University, Stillwater, Oklahoma.

1. Letter from Donald V. Hammond and Bernard Carreau, Acting Undersecretaries for Domestic Finance and International Trade, U.S. Dept. of Commerce, to John Mogg, Director General for EU Commission's Internal Market Directorate-General (Mar. 23, 2001), *available at* the EU's Web site, http://europa.eu.int/comm/internal_market/ (last visited Oct. 30, 2001) (seeking delay in the adoption of a Safe Harbor Agreement Art. 26 avenue–distinguished from the Art. 25 "safe harbor" list avenue—for meeting the requirements of the 1995 EU Data Privacy Directive and allowing EU data transfer to third countries; complaining that the EU's proposed contract clauses would add "duties and liabilities that are not found in" EU Directive 95/46/EC). In March 2001, the EU Commission voted unanimously, 14-0 with one abstention, to reject the U.S. Treasury and Commerce Department's request for delay, and referred the question to the EU Parliament, whose counsel the Commission had ignored in adopting the Safe Harbor Agreement of July 2000.

> The EU's data-privacy efforts for e-commerce could cause "imposition of one of the largest free trade barriers ever seen."
>
> – Representative Billy Tauzin, Chair of U.S. House of Representatives Committee on Energy and Commerce, Mar. 8, 2001.[2]
>
> The Senate today approved and sent on to the President an anti-terrorism package that would dismantle many privacy protections for communications and personal data. Many of the provisions are not limited to terrorism investigations, but would apply to all criminal or intelligence investigations. "This bill has been called a compromise," said Jerry Berman, CDT Executive Director, "but the only thing compromised is our civil liberties."[3]
>
> – Center for Democracy and Technology, Oct. 25, 2001.
>
> "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or *abridging the freedom of speech*, or of the press; or the right of the people peaceably to assemble, and to petition the Government for the redress of grievances."
>
> – U.S. Const. amend. I (emphasis added).

I. INTRODUCTION

Recent advances in computer technology present an information explosion to global society within an ever-broadening world of e-commerce, heralding the miracle of almost instantaneous data transmission throughout the world. The very same rapidly changing technology threatens serious invasions of personal and financial privacy, including computer fraud. Communications technology is necessarily intrusive and, spurred on by international efforts to ferret out terrorism as a result of the September 11, 2001, attacks on the United States, will become even more so. As a consequence of the attacks, throughout these pages we draw a

---

2. Quoted in Peronet Despeignes and Deborah Hargreaves, *The Americas: U.S. Criticises EU on Data Privacy,* FIN. TIMES (London), Mar. 9, 2001, at 12 (EU Data Privacy restriction not yet imposed on any U.S. company or Web site of consequence but, according to Rep. Tauzin, could lead to effective imposition of a "de-facto privacy standard on the world").

3. Center for Democracy and Technology, *at* http://www.cdt.org (last visited Nov. 4, 2001).

sharp distinction between governmental surveillance of e-commerce, necessitated perhaps by national-security imperatives, and invasive business practices aimed merely at mining the lucrative Internet market.[4] The U.S. Antiterrorism or so-called Patriot Bill approved by the U.S. Senate with one lone dissent on Thursday, October 25, 2001,[5] grants broad governmental safeguard powers to survey e-mail communications and even to prosecute immigrants for vague associations with suspected terrorists. The Bill, containing a sunset clause for expiration only after four years, has been immediately criticized by civil libertarians as overly broad.[6]

Although governmental intrusion into individual privacy is beyond our intended subject matter, this article on informational privacy is nevertheless written in the shadow of September 11. If anything, the terrorist attacks have increased use of the Internet to seek personally identifiable or identified information about individuals. The term "personal data" is used here as it is in Europe, to mean data either identified or identifiable to a particular individual.

Focusing on invasive business practices, the ever-watchful popular press is not unaware of the threat to personal privacy, and has repeatedly

---

4. Of the fifteen EU countries, post-WWII Germany has been by far the sternest protector of the right to personal privacy in the western world, with France also having very strong privacy laws; see, e.g., Case 11/1970, Internationale Handelsgesellschaft mbH v. Einfuhr-und Vorratsstelle für Getreide und Futtermittel ("Solangewie I") 1970 E.C.R. 1125, *infra* note 226. As investigations begin to reveal that the Al Qaeda plot to bomb symbols of U.S. power may have been hatched or at least furthered in part by money movements taken by foreigners in relative personal privacy inside Germany, a hue and cry will inevitably rise to clamp down on terrorist cells working inside the EU by enlarging the role of cyber-police and increasing surveillance of personal data. The U.S. will no doubt point to Germany's laxness in watching the private actions of its citizenry—and guests—as good reason for the U.S. to take a step backward and restrict data-privacy-protection in the U.S. Hence, our insistence in these pages on distinguishing between *government* surveillance and *business* or commercial intrusions.

5. Antiterrorism Bill, H.R. 3162, 107th Cong. (2001). A new European Convention on Cybercrime, to which the U.S. is a signatory, was opened for signatures on November 23, 2001 at Budapest. European Treaty Series no. 185. The Center for Democracy and Technology issued a press release on the Antiterrorism Bill on October 25, 2001, *at* http://www.cdt.org (last visited Nov. 4, 2001). Other privacy watchdogs decrying invasions of privacy are the Electronic Privacy Information Center, Washington, D.C., at http://www.epic.org; and the Privacy Rights Clearinghouse, San Diego, California.

6. Even Robert Novak on Cable Network News' (CNN's) "Capital Gang," no left-wing "liberal," described the "Patriot" or Antiterrorism Bill as a Federal Bureau of Investigation's "dream" statute. For further information see http://www.cnn.com (last visited Oct. 29, 2001). *See* N.Y. TIMES, Oct. 26, 2001, at A-1, B-6 (highlighting major provisions of the Antiterrorism Statute, signed by the President into law).

warned, long before September 11, of the inadequacy of legal safeguards in place to protect on-line data privacy. Consider, for instance, PCWorld, Business Week, Consumer Reports, and Time, *inter alia*, which have run alarming stories about the threats posed to individual privacy by on-line Web site practices, some stories published even a year after the effective date of the EU-U.S. Safe Harbor Agreement (July 21, 2000)[7] discussed below.

Since 1995, U.S. regulators themselves have noticed the potential threat to personal-data privacy posed by e-commerce, especially the FTC which is now charged with safeguarding individual and commercial on-line privacy. The FTC began studying the matter in earnest only in 1995,[8] by no mere coincidence the same year in which the EU enacted its data privacy directive, Directive 95/46/EC. The FTC issued its first on-line privacy report to Congress in 1998,[9] proposing guidelines only for industry

---

7. *On-line Privacy–It's Time for Rules in Wonderland*, BUS. WK., Mar. 20, 2000, at 83; *Big Browser Is Watching You*, CONSUMER REP., May 2000 at 43-51; *Net Privacy Now*, PC WORLD, June 2000, at 103; *Who Can See Your Medical Records?*, CONSUMER REP., Aug. 2000, at 628-33; Adam Cohen, *Internet Insecurity*, TIME, July 2, 2001, at 44.

8. The major FTC reports to Congress on on-line privacy: June 1998, July 1999, and May (and June) of year 2000 are available at http://www.ftc.gov. The FTC's first report, issued in June 1998 as *Privacy On-line: A Report to Congress,* found that 92% of commercial Web sites collected personal data from consumers but only 14% of those disclosed such practices to consumers. The FTC's 1999 report, issued in July 1999 as *Self-Regulation and Privacy On-line: A Federal Trade Commission Report to Congress,* discussed a disturbing survey from Georgetown University on personal-privacy invasions. In December 1999, the FTC formed an Advisory Committee on On-line Access and Security. The May 2000 FTC Report recognizes the inadequacy of recent attempts at industry self-regulation and is entitled *Privacy On-line: Fair Information Practices in the Electronic Market place: A Federal Trade Commission Report to Congress.* It recommends comprehensive federal privacy legislation to protect consumer on-line privacy for consumers not covered by COPPA, i.e., for consumers aged over thirteen years. In June 2000, the FTC issued a fourth report, *On-line Profiling: A Report to Congress*. Then, on March 31, 2001, the FTC held a workshop on *The Information Marketplace: Merging and Exchanging Consumer Data* which is available at http://www.ftc.gov. Sen. Hollings introduced S. 2606, the Consumer Privacy Protection Act of 2000, to the Senate the day after issuance of the May 22, 2000 FTC Report. His bill tracks the FTC proposals and decries "the constant assault on citizens' privacy by the denizens of the private market-place." The Consumer Privacy Protection Act of 2000, S. 2606, 106th Cong. (2002). Senators McCain and Kerry introduced S. 2928, *The Consumer Internet Privacy Enhancement Act,* on July 26, 2000. Eight privacy bills were introduced in the 106th Congress. For data-privacy bills introduced in recent congressional years, see http://www.cdt.org/privacy.

9. *Privacy On-line: A Report to Congress*, FTC REPORT, June 1998 (proposing that on-line business self-regulate by adopting practice codes or guidelines so that *consumers* would receive: (1) notice of the privacy policies of the on-line business which collects consumer

self-regulation so as to achieve fair information practices in consumer transactions. Also in 1998, the FTC filed its first complaint under FTC Act section five[10] against an on-line business for having breached its own stated privacy policy.[11] Two years later, the FTC's 2000 report to Congress noted

---

data; (2) access to their own personal data collected and stored by the on-line business; (3) choice in whether personal consumer data could be sold or otherwise disseminated to third parties; (4) assurance of security measures taken to ensure personal-data privacy; and (5) some sort of enforcement mechanism for violation of their right to personal-data privacy. These are called Fair Information Practices (FIPs)). More information is available at http://www.ftc.gov.

10. It is unclear whether the U.S. Congress has granted competence to the FTC over U.S. companies' compliance with the EU Safe Harbor Agreement reached in July 2000. *See* F.T.C. Act § 5, 15 U.S.C § 45(a) (1914), originally covering only unfair methods of competition, as amended by the FTC Act Amendments (Wheeler-Lea Act) of 1938, 49 U.S.C. §§ 3, 5(a) (1938), giving the FTC jurisdiction over unfair or deceptive trade practices, on the rationale that consumers benefit by increased competition. The Safe Harbor Agreement, EU Commission Decision 2000/520EC, 2000 O.J. (L 215 7), states that it applies only to firms coming under the regulatory jurisdiction of the U.S. FTC and Department of Transportation. Now, the act of a business' registering itself on the U.S. Department of Commerce's "Safe Harbor" list arguably brings the business within the jurisdiction of the FTC allowing the FTC to sue the business for violating its own stated privacy policy.

11. Also in the year 1998, Congress enacted the Child On-line Privacy Protection Act (COPPA) requiring the FTC to adopt rules and regulations for on-line consumer transactions of children (aged 13 and under). In re GeoCities, File No. 9823015 (F.T.C. 1998) (reaching consent judgment for FTC's first enforcement action brought under COPPA, judgment in August 1998, prohibiting further misrepresentation and mandating clear notice to consumer customers of on-line privacy policies). On February 13, 2002, the FTC announced its fifth enforcement action under its COPPA Rule (effective in Apr. 2000) and stated the FTC's intent to prosecute COPPA violations rigorously. The American Popcorn Co. agreed to pay $10,000 to settle FTC charges of violating the FTC's COPPA Rule, by collecting personal information from children on its "Jolly Time" Web site, aimed at children, without obtaining parental consent. The settlement also barred future violations of the COPPA Rule. The complaint and settlement were filed by the Department of Justice at the request of the FTC in U.S. District Court for the Northern District of Iowa, Western Division, in Cedar Rapids. *See also* F.T.C. v. Liberty Financial Cos. and F.T.C. v. ReverseAuction.com. In these cases—*GeoCities, Liberty, ReverseAuction*, and *American Popcorn*—there was a finding of either deceptive or unfair trade practices, involving in some a violation of a stated privacy policy, which is a "deceptive" practice under F.T.C. Act § 5; but in none does the FTC assert overall jurisdiction to require a company to adopt a data-privacy policy. The FTC has questioned whether it even has competence to require business adoption of privacy policies. Letter from then-Chair of the FTC, Robert Pitofsky, to John Mogg, Director, Directorate General XV of the European Commission (July 14, 2000): "For this reason, the Federal Trade Commission stated in Congressional testimony that additional legislation probably would be required to mandate that all U.S. commercial Web sites directed toward consumers abide by specified fair information practices." (Citing *Consumer Privacy on the World Wide Web,* Before the

"significant consumer privacy concerns" arising from "the prevalence, ease, and relatively low cost" of collecting and transferring personal data.[12] Conceding in the May 2000 Report of the FTC that industry self-regulation was inadequate to address the on-line privacy issue, the agency dramatically reversed its prior favorable position on self-regulation and called for federal privacy legislation.

For myriad historic, political, and cultural reasons, some of which are discussed shortly, the European Union (EU) not surprisingly is far ahead of the U.S. in the matter of on-line privacy protection. Consumers in the EU now have ready access to data about themselves, including the right to alter their data, or to purge their personal data after the absolutely necessary time for data life has passed, and the right to "opt-in" affirmatively to being covered in the first place. Consumers in the U.S. generally have only the chance, if at all, to "opt-out" of coverage, and little power to prevent personal data in public records from being collected and re-sold to third parties without their knowledge and consent. American businesses generally have not wanted to provide consumers the "opt-in" provision. As an example of "opt-out," the big three credit-data reporting companies in the U.S. (Experian, TransUnion, and Equifax), now offer telephone numbers or addresses to which consumers may report their desire to opt out of having their personal data reported to third-party marketers. This "opt out" possibility begs the question, though, of how the "big three" credit-checking companies initially acquired, and retained, the consumer's data.

The EU, moreover, is determined to extend its privacy initiative beyond its own borders, through the EU's 1995 Data Privacy Directive (Directive 95/46/EC). In addition to the EU Directive's requiring its own member states to implement national legislation ensuring personal data privacy, guaranteeing the right of privacy to EU citizens within their member states, the Directive demands privacy protections for EU citizens

---

Subcommittee on Telecommunications, Trade and Consumer Protection of the House Committee on Commerce, United States House of Representatives, July 21, 1998, *available at* http://www.ftc.gov/os/1998/9807/privac98.htm (last visited Apr. 8, 2002); U.S. West, Inc. v. F.C.C., 182 F.3d 1224 (10th Cir. 1999), *cert. denied*, 530 U.S. 1213 (2000). (The FTC has no right under First Amendment to prohibit Federal Communications Commission's opt-out procedure, although in *obiter dictum* court says the U.S. Congress could invalidate FCC's opt-out plan and require opt-in procedure requiring action not by consumer but by collector and user of personal data). The FTC's Web site is at http://www.ftc.gov. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into its Consumer Sentinel on-line database available to foreign and domestic civil and criminal law enforcement agencies.

12. Final Report of the FTC Advisory Committee on Online Access and Security (May 2000), *at* http://www.ftc.gov/acoas/papers/finalreport.htm.gov (last visited May 20, 2002).

from on-line businesses around the world, including those domiciled in the U.S. Article 25 of the Directive plainly says this about onward transfer: "[EU] Member States shall provide that the transfer to a third country of personal data . . . may take place only if . . . *the third country . . . ensures an adequate level of protection*" (emphasis added).[13] As of February 1, 2002, only three non-EU countries, Hungary, Switzerland, and later U.S. NAFTA-partner Canada, have received certification as countries to which EU data can be freely sent.[14] Not far behind are Hong Kong, Australia, New Zealand, and Argentina, as well as Poland which hopes to join the EU shortly.[15]

As a measure *sui generis* from country-certification, the EU and the U.S., after extensive high-level government negotiations, hammered out a compromise labeled the Safe Harbor Agreement on July 21, 2000, which allows onward transfer of EU data to U.S. companies complying with Safe Harbor requirements. U.S. business has decried the possible lack of jurisdiction in the U.S. FTC over Safe Harbor matters; the EU Parliament's objection that the EU Commission's approval of Directive 95/46/EC predated the Safe Harbor Agreement; and the effectively extraterritorial impertinence of the EU Data Privacy Directive itself.[16]

---

13. The 1995 EU Data Privacy Directive is Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) 0031-50. The Directive is available at http://europa.eu/int/comm/internal_market/en/dataprot/law/index.htm. The Safe Harbor Agreement, Comm. Dec. 2000/520/EC, 2000 O.J. (L 215) 7. The Safe Harbor Agreement compromise between the EU and the U.S. leaves gaps. Its progenitor, the 1995 EU Data Privacy Directive, itself, after its three-year run-in period, is "directly effective." Direct effectiveness of an EU directive, although rare, means generally that private citizens (consumers, here) have *locus standi* to bring a private right of action in their own national courts against violators of the Directive, including against EU governments (called "vertical direct effectiveness" in the EU) and against private companies (called "horizontal direct effectiveness" in the EU). Early EEC cases establishing the principle of direct effectiveness include Defrenne v. Sabena Airlines, Case 80/70, 1971 E.C.R. 445.

14. Directive 95/46/EC prohibits the transfer of personal data to non-EU nations that do not meet the European "adequacy" standard. Hungary, Switzerland, and later Canada were certified by the EU as third-party states to which onward transfer from the EU of personal data could be freely made. *See* http://www.export.gov (last visited Feb. 1, 2002); http://europa.eu.int/comm/internal_market/en/dataprot/adequacy/index.htm (last visited Feb. 1, 2002); and http://www.export.gov/safeharbor (last visited Feb. 1, 2002).

15. Hungary, Switzerland, and Canada are listed at http://europa.eu.int/comm/internal_market/en/dataprot/adequacy/index.htm (quoting EU Commission Decisions on the adequacy of the protection of personal data in third countries).

16. U.S. West, Inc. v. F.C.C., 182 F.3d 1224 (10th Cir. 1999). U.S. resentment of the extraterritorial provision (Art. 25) in the EU's 1995 Data Privacy Directive almost beggars

Nevertheless, U.S. businesses have ostensibly begun to comply, motivated presumably by their wish to maintain favorable commercial relations with the huge European market, now the world's largest trading bloc.[17] U.S. companies under the jurisdiction of the FTC and the U.S. Department of Transportation,[18] and in compliance with the Safe Harbor Agreement are listed on the Safe Harbor list maintained by the Department of Com-

---

reason in light of such U.S. extraterritorial legislation as the Helms-Burton Statute. *Cf.* regarding U.S. anger, some U.S. positions asserting extraterritorial jurisdiction: The Helms-Burton Act or Cuban Liberty and Democratic Solidarity [Libertad] Act of 1996, 22 U.S.C. §§ 6021-6091, 35 I.L.M. 357 (1996); The Iran and Libya Sanctions Act, 35 I.L.M. 1273 (1996).

17. U.S. software giant Microsoft, for example, announced in May 2001, its intention to sign onto the Safe Harbor list. Deborah Hargreaves, *Microsoft to Adopt EU's Data Privacy Rules*, FIN. TIMES (London), May 16, 2001, at 12. Protection of personal data privacy offered by U.S. business may be more chimera than reality. Having to "opt out" of allowing personal-data exchanges among banks, e.g., is too cumbersome a requirement for most U.S. consumers to meet. Sen. Hollings in introducing S. 2606, The Consumer Privacy Protection Act of 2000, before the U.S. Senate on May 23, 2000, felt that an "opt-out" policy was not designed fully to inform the consumer but to encourage business to bury their privacy policies in boilerplate thereby dissuading the consumer from opting-out. The Consumer Privacy Protection Act of 2000, S. 2606, 106th Cong. (2002). On "opt-out" procedures, see *U.S. West, Inc.*, 182 F.3d 1224. To purists it is always constitutionally questionable whether federal administrative agencies such as the FTC violate the U.S. Separation of Powers doctrine when enacting and enforcing administrative rules and regulations instead of Congress' enacting identical statutes.

18. U.S. Safe Harbor jurisdiction is thought to exist in the FTC (which includes deals affecting consumers but excludes provision of financial services) and the Department of Transportation. The Gramm-Leach-Bliley Bill imposes privacy-protection provisions on banks and financial institutions, while at the same time lifting the old Glass-Stegall limitations on banking's ability to offer collateral services such as financial advice. As federal administrative agencies, the FTC and the Department of Transportation can issue "Cease and Desist" (C&D) orders (administrative quasi-injunctions) against noncompliance. The U.S. Government's Web site for Safe Harbor information is available at www.export.gov, to which U.S. companies may self-certify their compliance with Safe Harbor Principles. The Safe Harbor List is maintained by the U.S. Department of Commerce, which does not guarantee the accuracy of the information self-supplied by industry; U.S. organizations could begin signing up to the safe harbor list at www.ita.doc.gov/ecom beginning on Nov. 1, 2000, by inputting their own information into the Web site or by writing: The U.S. Dept. of Commerce, Attention: Safe Harbor Registration, Room 2009, Washington, D.C. 20230. A year later, as of November 1, 2001, over 100 companies had certified themselves as compliant and placed themselves on the Safe Harbor list. *See* http:/www.ita.doc.gov/td/econ/FRN2.htm. The U.S. Government maintains a Safe Harbor workbook to assist businesses in compliance for their privacy policies and practices with the Safe Harbor Agreement. This workbook is available at http://www.export.gov/safeharbor/sh_workbook.html. In addition, the Government provides a Safe Harbor Overview which may be accessed at http://www.export.gov/safe harbor/sh_overview.html.

merce. A company "self-certifying" and listing itself on the Safe Harbor roll simultaneously subjects its privacy policy to enforcement by the FTC.[19]

Subsequent to execution by the EU and the U.S. of the Safe Harbor Agreement reached in late July 2000, the EU Commission has adopted a set of standard form contract clauses (model contract clauses) warranting personal data privacy.[20] Article 26 of Directive 95/46/EC offers use of these clauses in business deals as an alternative to conformance with the Safe Harbor provision envisioned in Directive Article 25. U.S. companies inserting these standard clauses promulgated by the EU into their contracts with EU-connected companies can satisfy the EU Directive through compliance with its Article 26 instead of Article 25. U.S. business then would be able to comply with EU demands on a contract-by-contract basis.

---

19. See http://www.ita.doc.gov/ecom (last visited Nov. 4, 2001).

20. On January 19, 2001, the EC Commission released another draft of model contractual provisions proposed for U.S., and other third-country businesses to use (in lieu of complying with the Safe Harbor Agreement by voluntarily listing themselves on the "Safe Harbor" list maintained by the U.S. Dept. of Commerce). The Export Portal of Commerce on the Web contains: Safe Harbor Overview; Safe Harbor Documents; Safe Harbor Workbook; Safe Harbor List; Certification Information; Certification Form; Model Contract Information; Data Privacy links; Historical Documents & Public Comments; and Privacy Statements. The Export Portal is available at http://www.export.gov/safeharbor/sh_modelcontract.html. The U.S. Department of Commerce provides instructive information on the Web about the Standard Contractual Clauses which are located at http://www.export.gov/safeharbor/sh_overview.html. The EU provides information at http://europa.eu.int/comm/internal_market and an EU e-Mail address: markt-A5@cec.eu.int. *See Standard Contractual Clauses: Proposed by the EU Commission*, Draft Commission Decision on Standard Contractual Clauses for the transfer of personal data to processors established in third countries (Oct. 1, 2001 version). The European Commission has notified to Member States (management Committee established by Article 31 of the Directive 95/46/EC) a Draft Commission Decision on standard contractual clauses for the transfer of personal data to data processors established in third countries together with the favourable opinion issued by the Working Party on the protection of individuals (Expert data protection group established by Article 29 of the Directive where National Data Protection Authorities are represented). This draft (Oct.1, 2001 version) is the final result of the intensive consultations carried out with the Member States and the Data Protection Supervisory Authorities. Since April 2001, several meetings have been devoted to discussing this issue with the Member States and the Article 29 Working Party. Following the public consultation launched in this Web site on July 3, 2001, contacts and meetings with business and consumer associations have taken place. The European Parliament has been kept informed in accordance with the arrangements agreed for the implementation of Council Decision 1999/468/EC. Pursuant to the procedure laid down in Article 31 of the Directive 95/46/EC, Member States were invited to deliver an opinion at the meeting to take place on Oct. 23-24, 2001.

Taking early umbrage at these model or standard contract clauses advanced by the EU, in March 2001, the new Bush Administration signaled its wish to "delay" the EU's elaborations made after and upon the July 2000 Safe Harbor Agreement. Specifically, the George W. Bush Administration labeled "burdensome to U.S. multinational business" the EU's effort under Article 26 of the 1995 Data Privacy Directive to draft and propose standard contract clauses which business could use as an alternative to becoming qualified to lie within the "safe harbor" provisions of Article 25 of the Directive.[21] As the EU Commission has explained the difference between, one, a company's qualifying under the Safe Harbor provision (implicating Directive Article 25) and, two, using the EU-adopted standard contractual clauses: "In general lines, U.S.[-]based companies receiving data from the EU under the standard contractual clauses benefit from a different Article of the Directive (Article 26 instead of Article 25 for the Safe Harbor) and they must guarantee the enforcement of individuals' rights with a different approach, which has to be the same for all data importers irrespective of their geographical location."[22]

---

21. Letter from U.S. Dept. of Commerce and U.S. Treasury Dept. to the EU Commission, evaluating the Safe Harbor Agreement as a threat to transatlantic e-commerce for potentially burdening Web site operators with red tape. Charles Arthur, *Bush Wants to Scrap Deal on Internet Privacy*, THE INDEP. (London), Mar. 31, 2001, at 11. "America is pressing for a delay—at least—of the treaty hammered out last year after months of talks between the Clinton administration and the European Union. . . . The move mirrors the announcement earlier this week that the United States will not implement the Kyoto treaty on tackling the pollution that causes climate change, and suggests that America is becoming increasingly aggressive in pushing its agenda on the world." *Id.*

22. Letter from EU Commission, John F. Mogg, Director General of the Internal Market Directorate-General of the EU, to Ms. Maja Wessels, EU Committee of the American Chamber of Commerce in Belgium (Mar. 2001), *available at* http://europa.eu.int/comm/internal_market (last visited Oct. 30, 2001). "[T]he Draft Commission Decision does allow U.S. based companies to use the relevant Safe Harbor Principles and Frequently Asked Questions as substantive provisions on data protection. However, as was anticipated in the exchange of letters that preceded the Safe Harbor, the fact that U.S.-based importers under the clauses are not *harborites* has some consequences that need to be properly addressed by the Draft Commission Decision. For instance, U.S. importers under the [standard contract] clauses do not publicly declare their adherence either to the Safe Harbor rules or to the Safe Harbor list handled by the Department of Commerce. U.S. importers under the [standard contract] clauses do not submit themselves to a private sector dispute resolution mechanism or the supervision of the Federal Trade Commission or equivalent body. . . The standard contractual clauses will obviate the need for national authorisations within the meaning of Article 26(2) of the Directive." *Id.* Article 26(4) of Directive 95/46/EC defines the meaning and effects of the standard contractual clauses approved by the EU Commission. The Member States must comply with the Commission's

The strategic policy manager of the UK information commissioner's office has opined, "The safe harbour system is meant to be simple, cheap and easy for U.S. firms to sign up to. If a company like Hewlett-Packard could do it, why couldn't others?" The data-protection compliance officer in Britain for the credit-checking company Experian has prophesied, "If the U.S. tears up the safe harbour agreement, it takes us back to the situation where every individual person has to agree before their data can be passed to a company in the U.S. Removal of the Safe Harbor Agreement would increase the difficulty of EU businesses' trading data with U.S. companies, causing the potential loss of billions of dollars in trade." The Director of the UK's Direct Marketing Association has said, "Companies in Europe find that data privacy law doesn't get in the way; but you have to be a lot more transparent when you ask an internet user to provide data . . . and give them the option for that data not to be used."[23]

The George W. Bush Administration's March 2001 letter to the EU Commission has evoked rumors of a coming trade war between the EU and the U.S. over the data privacy issue. U.S. critics characterize EU privacy efforts as a "direct reversal" of the worldwide trend for global trade liberalization.[24] If the EU brings action against the U.S. for retrenchment from the Safe Harbor Agreement achieved late in the Clinton Administration,[25] the fear is that the U.S. will consider EU action an impermissible trade sanction imposed on the U.S., causing the U.S. to retaliate against EU firms operating within the U.S. The corresponding EU fear is that privacy restrictions imposed within the EU and not within

---

Decision adopting these clauses, "i.e., they must accept as adequate[,] contracts complying with this model." *Id.*

23. Arthur, *supra* note 21, at 11. Mr. Ian Bourne is quoted from the UK information commissioner's office. The data-protection compliance officer in Britain for the credit-checking company Experian is Mike Bradford.

24. Representative Billy Tauzin, Chair of U.S. House of Representatives Committee on Energy and Commerce, Mar. 8, 2001. *See supra* note 2 and accompanying text. "[W]e share the concern of a number of multinational firms that [EU] adoption of the proposed standard clause will introduce uncertainty about the use of contracts. . . . The proposed standard clauses are not a workable model. They impose unduly burdensome requirements that are incompatible with real world operations. While revisions and improvements have been made since the [EU presented the] standard contract clauses . . . for comment in September 2000, the revision process has not been transparent to those seeking participation." Letter to EU Commission simultaneously released to the press from the U.S. Dept. of Commerce, Mar. 23, 2001.

25. President Clinton supported a strong personal-privacy policy. President William Jefferson Clinton, Remarks by the President to the Forum on Communications and Society on the Information Age Agenda, Address Before the Meeting of the Aspen Institute (Mar. 3, 2000).

the U.S. will place European firms at a competitive business disadvantage to the U.S., with multinational firms choosing to operate in the looser regulatory environment of the U.S.[26]

The issue at hand is far broader than mere compliance with the EU's extraterritorial summons to preserve and protect individual and commercial on-line data privacy. Indeed, at its root the issue seems not so much the direct challenge by the EU to supremacy of U.S. law within the U.S., but the clash within the U.S. between free speech, on the one hand, and a U.S. privacy policy, on the other hand. This privacy policy needed for consumers regarding their personal data is stalked by U.S. judicial interpretations that have already rendered an unacceptable assault on fundamental notions of privacy.

Will the *ius gentium* (law of nations) regarding personal-data privacy be domestic U.S. law, "written," as it were, as a reflection of the EU-U.S. safe harbor accord and subsequent transactions? Will it, more likely, be written ultimately by the European Union's determined effort to put teeth into Directive 95/46/EC? In other words, will the EU Data Privacy Directive set a *de facto* privacy standard for the western world? Or will the *ius gentium* be a hybrid of the practices of the several large commercial countries' data-privacy practices?

Will the "international law" of data privacy be truly an international law in the sense of international treaties and customs and practices generally observed by civilized sovereign nations governing their relations *inter se*, such as affording places of asylum, curbing certain barbarous practices in war, and protecting ambassadors from attack in foreign states? Probably not, we predict, at least for the next few decades. The *ius gentium* under Roman law was not true international law in this latter sense. "Actually it was Roman law adapted to Roman sovereignty, and designed to govern the peoples of Italy and the provinces without giving them Roman citizenship and the other rights of the *ius civile.*"[27] The Romans decreed, "*Non erit alia lex Romae, alia Athaenis; alia nunc, alia posthac; sed et omnes gentes, et omni tempore, una lex, et sempiterna, et*

---

26. Andy McCue, *E-Business; The U.S. Harbours Data Privacy Doubts*, COMPUTING, June 20, 2001; *U.S. Throws Down the Gauntlet Over E-Privacy: An E-Commerce Trade War is Looming as a Transatlantic Data Privacy is Challenged by the New U.S. Government*, COMPUTING, Mar. 27, 2001. On the privacy issue, sometimes left meets right. William Safire, *Stop Cookie-Pushers*, N.Y. TIMES, June 15, 2000, at A27.

27. WILL DURANT, THE STORY OF CIVILIZATION: PART III, CAESAR AND CHRIST 404 (Simon and Schuster 1944). DAVID J. BEDERMAN, INTERNATIONAL LAW IN ANTIQUITY, (Cambridge Univ. Press 2001) (studying the earliest developments of the law of nations); PETER STEIN, ROMAN LAW IN EUROPEAN HISTORY (Cambridge Univ. Press 1999) (delineating how Roman law lives on).

immortalis continebit." The English translation is, "There will not be one law at Rome, another at Athens; one law now, another hereafter; but one eternal and immortal law shall bind together all nations throughout all time."[28]

And just so should the pertinent *ius gentium* become EU law on individual data privacy rights, neither the less perceptive, relatively myopic, U.S. law nor some hybrid reached between the two regimes. The momentum is with Europe on protecting data privacy and outlawing the death penalty as aspects of the fundaments of human rights. European countries' refusals to extradite to the U.S. suspected 9/11/01 terrorists unless the U.S. grants concessions concerning restraint from assessing the death penalty highlight this momentum too.[29] Western Europe's post-war enlightened practices respecting the individual will necessarily be imported eventually into its former colonies in North America.

Discussion of the EU-U.S. on-line data privacy paradigms reveal a collision of vital ideas concerning constitutional rights, a collision whose thread weaves strongly throughout this topic. Yet, with U.S. businesses at least outwardly hurrying to conform to the 1995 EU Data Privacy Directive (a harmonizing directive which became fully effective in 1998 after a three-year run-in period), the actual practice of U.S. business vis-à-vis data privacy will perforce change the context of U.S. legal analysis of personal data-privacy rights, and of the right of "commercial speech" created judicially under the First Amendment to the United States Constitution. For in today's global e-commerce, the speech forum for commercial speech necessarily shifts from "within the nation" to "among nations," a venue the constitutional parameters of which the U.S. Supreme Court, despite such recent cases as *Hill v. Colorado*,[30] cannot prescribe for nations other than the U.S.

It is not our purpose here to offer another nomography on U.S. privacy. We do not attempt a detailed discussion of the inadequacy of U.S.

---

28. BLACK'S LAW DICTIONARY 1201 (4th ed. 1957).

29. Ellen Hale, *Death Penalty Could Affect Extradition to U.S.*, USA TODAY, Oct. 10, 2001, *available at* http://www.usatoday.com/news/attack/2001/10/03/extradite-usat.htm. "The United States might have to sacrifice the death penalty if it wants to extradite and try suspected terrorists arrested in Europe." *French Court Backs Kopp Extradition* (June 28, 2001), *available at* http://www.cnn.com/2001/WORLD/europe/06/28/france.kopp. "Three French judges have recommended the extradition of one of the United States' most wanted fugitives - as long as he will not face the death penalty." Mark Warren, *The Death Penalty in Canada: Facts, Figures and Milestones, available at* http://www.ccadp.org (last visited Apr. 8, 2002).

30. Hill v. Colorado, 530 U.S. 703 (2000); Lorillard Tobacco Co. v. Reilly, 533 U.S. 525 (2001).

legal protection of personal privacy[31] that eventually led to patchwork congressional enactment of national statutes such as the Identity Theft and Assumption Deterrence Act (1998), COPPA (1998),[32] and the Electronic Signatures Act,[33] and various other national laws containing isolated privacy provisions,[34] as well as state privacy laws and constitutions; or to offer extensive analysis of these piecemeal acts themselves.[35] Nor do we

---

31. *See, e.g.*, Kurt M. Saunders & Bruce Zucker, *Counteracting Identity Fraud in the Information Age: The Identity Theft Deterrence Act*, 8 CORNELL J.L. & PUB. POL'Y 661 (1999).

32. The Identity Theft and Assumption Deterrence Act of 1998, 18 USC § 1001(a) (2002); The Children's On-line Privacy Protection Act (COPPA) (covering children under 13 years of age or less), 15 U.S.C. §§ 6501-6505 (enacted Oct. 21, 1998 and effective Apr. 21, 2000). *See* Federal Trade Commission-Facts for Businesses, *How To Comply With COPPA*, *at* http://www.ftc.gov/bcp/con-line/pubs/ buspubs/coppa.htm (last visited Mar. 27, 2002). Pertinent FTC Regulations are at 64 Fed. Reg. 59911 (Nov. 3, 1999), as Part 312 of Title 16 of the C.F.R. The Department of Health and Human Services (HHS) announced regulations on December 20, 2000, effective February 26, 2001, backing up the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (protections to be required for health care information) (to protect the medical records of U.S. patients). President Clinton announced at the release of the rules that these rules were "the most sweeping privacy protection ever written." The Bush administration postponed the effective date of the regulations to allow additional reviewing time. Parenthetically, it is nothing new for critics to complain that federal administrative agencies' rule-making powers represent an unconstitutional exercise of powers reserved to the legislature. *See*, e.g., W. Schiffbauer, *Congress Impermissibly Delegated Law-Writing Power to Executive Branch in Privacy Rule*, PRIVACY L. ADVISOR, Feb. 7, 2001, at 453.

33. The Electronic Signatures in Global and National Commerce Act (E-SIGN) of 2000, 15 U.S.C. § 7001 (2000). *See infra* note 58.

34. The 1970s marked new interest in privacy protection in the U.S., e.g., The Privacy Act of 1974, 5 U.S.C. § 552A, which regrettably applies only to data collection by the federal government. Another act of interest is The Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2510-2522, regulating government surveillance of telephone wires, cell phones, beepers and like technologies. The Family Educational Rights and Privacy Act of 1974 (FERPA), 20 U.S.C. § 1232(g) (West 2001)(known as FERPA or the Buckley Amendment), protects student educational privacy. Regarding FERPA, the Family Policy Compliance Office maintains a Web site at http://www.ed.gov/offices/ OM/fpco. Ironically, the 1970s marked a concomitant rise in the newly created constitutional right of Freedom of Commercial Speech. *See* Bigelow v. Virginia, 421 U.S. 809 (1975).

35. For that latitudinal view, we commend to the reader the Web sites of the EU, the U.S. FTC, and various U.S. and UK elected representatives and organized privacy watchdogs. For commentary on some of these privacy acts, see Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 IND. L. REV. 174 (1999) and Ronald J. Krotoszynski, Jr., *Identity, Privacy, and the New Information Scalpers: Recalibrating the Rules of the Road in the Age of the Infobahn: A Response to Fred H. Cate*, 33 IND. L. REV. 233 (1999) (suggesting that state statutes legislate that there is no property interest in personal data).

offer yet another detailed retelling of the events leading to the EU's intense interest in protecting the privacy of its citizenry which culminated in the 1995 Data Privacy Directive.[36] Instead, with the Safe Harbor Agreement of July 2000 acting as fulcrum, we consider the proposition that Western Europe is ahead of the U.S. in insisting upon and providing essential protection of individual privacy, particularly on-line privacy of personal information.

The sharp European contrast with the United States, especially in an era of potentially invasive technology, invites serious study and even emulation. The sincerest and safest form of imitation for civil libertarians would be a frank amendment to the U.S. Constitution guaranteeing the sanctity of personal data, subject to a safeguard clause allowing limited intrusions as demanded by the national interest.[37] A constitutional amendment would not be so subject to changing, even whimsical, judicial interpretation (according to the particular court's political or socio-economic composition, or interpretive philosophy) as might be a national privacy statute. Professor Joel Reidenberg has recommended that the U.S. sign an international treaty to be written so as to safeguard and make uniform the U.S. national data-privacy laws.[38] Such a treaty still might be declared unconstitutional by U.S. courts, though, making constitutional amendment still the optimal choice, albeit politically unlikely. Next best, we contend, but also subject to possible judicial findings of unconstitutionality, would be a comprehensive national privacy statute of the sort which is currently pending but stalled in the U.S. Congress and which tracks the language of the 1995 EU Data Privacy Directive and the subsequent Safe Harbor Agreement between the U.S. and EU.[39] Canada as an exemplar

---

36. The genesis of the Directive predates even the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data from the Organization for Economic Cooperation and Development. *See* Organization for Economic Cooperation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD Pub. and Info. Center 1980). The OECD is an organization formed post-World War II essentially for highly industrialized, western countries, as kind of a businessperson's elite club.

37. Article V of the U.S. Constitution allows two methods for amending the Constitution.

38. Joel Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, 38 HOUSTON L. REV. 717, 746 (2001).

39. Washington pundits predict that these national privacy bills are going nowhere in the current political climate. Just prior to September 11, 2001, the N.Y. Times headline "above the fold" pronounced: "Government Wary of Laws on Privacy." The text said, "Washington is not creating new laws and regulations that might restrict the use of cookies and other high-technology tools by businesses to monitor Internet users' activities. Some lawmakers say that the politics of privacy is so sensitive and complex that a deliberate

has recently enacted a comprehensive statute, the Personal Information Protection and Electronic Documents Act, to protect personal data gathered, used, or disseminated by organizations.[40]

II. U.S. DATA PRIVACY PARADIGM

A. U.S. Statutory Scheme

The term which best describes the U.S. approach toward overseeing "true" (not "false") commercial speech is self-regulation. Such self-supervision has in many cases proved highly effective, but only after the nudge given U.S. business by the 1995 EU Data Privacy Directive. Self-regulation has long allowed business to hold moot any need for national statutes preventing disclosure of personal data, although in limited cases public outcry has caused data-information companies to retreat from selling personal data.[41]

Yet in the specific area of data privacy, the U.S. approach has been sporadic and tenuous, and apparently inadequate for a problem manifesting serious international implications for the dissemination of private data

---

approach is best—but there is growing agreement that some kind of government action will eventually have to emerge. [Although Sen. Hollings of S.C.] has a strong interest in privacy, the Senate is currently bogged down in the appropriations process and other issues. The [Republican] leadership of the House has called for the debate to be refocused on the misdeeds of the government rather than those of companies." John Schwartz, *Government is Wary of Tackling On-line Privacy*, N.Y. TIMES, Sept. 6, 2001, at A-1.

40. The Personal Information Protection and Electronic Documents Act is available at the Privacy Commissioner of Canada Web site: http://www.privcom.gc.ca/legislation/02_06_01_e.asp.

41. The press wire reports that the U.S. House Banking Committee studied bank advertisements from eleven companies offering confidential information about their customers' bank accounts, finding that all eleven companies offered to sell these data for money; *see* http://www.newsbytes.com. Testimony before the House Banking Committee reported that the 1999 Gramm-Leach-Bliley Act had not been effective in curbing such privacy violations. 28 EUROPEAN NEWSLETTER 3 (CCH London Oct. 2000). Professor Cate cites flagrant abuses of personal data privacy contemplated by Equifax, Lotus, and Lexis-Nexis, including the selling of personal data collected by these companies. These sale plans were abandoned because of outraged consumer protest, which of course militates toward arguing that the market mechanism will work to regulate abuses of personal privacy. *See also, e.g.*, Cate, *supra* note 35, at 174 nn.1-6, 312. Cybercrime has become a major problem for e-commerce worldwide, causing the Council of Europe to propose an International Convention on Crime in Cyberspace, Article 14 of which reads: "Each Party shall take such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access a computer system or part of it and computer data stored therein . . . for the purpose of criminal investigation or proceedings."

(data which are identified or identifiable to a particular person).[42] In an admission of inadequate industry self-regulation, the FTC has recently characterized the U.S. approach to on-line data privacy as "sectoral,"[43] an approach representing an admixture of self-regulation, state and federal legislation, and regulation.

Two principal U.S. Supreme Court decisions, each relatively recent, offer a new U.S. "commercial speech" doctrine: *Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council* and *Central Hudson Gas & Elec. Corp. v. Public Service Comm'n.*[44] The *Central Hudson* test asks four cumulative questions: (1) was the commercial speech legal, truthful, and not misleading? (2) was the attempted regulation of commercial speech designed to advance a *substantial* governmental interest? (3) did the regulation in fact advance a substantial governmental interest? and (4) was there a reasonable relationship between the ends to be achieved by the regulation and the means of the regulation?[45] These questions offer a balancing test of public and business interests which grants "commercial speech" a lesser First Amendment protection than noncommercial speech.

A great deal of U.S. commercial speech is now, since 1975, judicially protected by the First Amendment.[46] For instance, germane to regulation of U.S. commercial practices on a continuing ad hoc basis is the U.S. Supreme Court's recent finding that advertising is commercial speech protected by the First Amendment against certain attempts at state regulation. Justice O'Connor found the state restrictions, which banned outdoor tobacco advertisements in the likely eyesight of teenagers and children, to violate the federal Cigarette Labeling Act and to "constitute nearly a complete ban on the communication of truthful information."

---

42. Stephen D. Hogan & Marsha Cope Huie, *EU Data Privacy and the U.S. Constitution—The U.S. Perspective*, EU FOCUS 1 (CCH London, Sept. 7, 2000).

43. U.S. Dep't of Commerce, *Safe Harbor Privacy Principles* (July 21, 2000), *available at* http://www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm.

44. Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748 (1976); Central Hudson Gas & Elec. Corp. v. Public Service Comm'n, 447 U.S. 557 (1980); Lorillard Tobacco Co. v. Reilly, 533 U.S. 525 (2001) (reaffirming the *Central Hudson* test as U.S. law for commercial speech).

45. *Central Hudson Gas & Elec. Corp.*, 447 U.S. 557. In United States v. United Foods, Inc., 533 U.S. 405 (2001), the dissent criticizes the majority's opinion as leading to doctrinal uncertainty concerning "compelled" commercial speech, with the majority's holding that business cannot be compelled by governmental regulation to underwrite speech with which it disagrees. This decision is expected to support increased challenges by business to economic regulation. *See infra* note 158.

46. Bigelow v. Virginia, 421 U.S. 809 (1975). *See also* Tamara Piety, *Merchants of Discontent: An Exploration of the Psychology of Advertising, Addiction, and the Implications for Commercial Speech*, 25 SEATTLE U. L. REV. 377, 450 (2001).

This case on tobacco advertising, *Lorillard Tobacco Co. v. Reilly*,[47] really carves no new law because it is in line with High Court precedent beginning in 1975 with the case of *Bigelow v. Virginia*.[48]

Bigelow was first to hold U.S. commercial speech (advertising) to be within the ambit of First Amendment protection. The law after *Bigelow* has developed in an unfortunate way, as commercial speech (not political speech) articulated only in the interest of mercantilism, and discounting the interest of the commonwealth, can ultimately only have a deleterious

---

47. *Lorillard Tobacco Co.*, 533 U.S. 525. The Court held, in a 5-4 decision, that the local (Boston) and state regulation of tobacco advertising is preempted, concerning cigarette advertisements, by the Federal Cigarette Labeling and Advertising Act. The Federal Act specifically states that "no requirement or prohibition based on smoking and health shall be imposed under state law with respect to the advertising or promotion of any cigarettes[,]" packaging of smokeless tobacco and cigars in compliance with the health-warning requirements of the federal statute. 15 U.S.C. § 1334 (2001). The usual four dissentients, Justices Stevens, Ginsburg, Breyer and Souter, would have held that Congress did not intend the 1965 Act fully to preempt state and local regulation of cigarette advertising but merely "a narrow set of content regulations." "Noble ends do not save a speech-restricting statute whose means are poorly tailored," said Stevens J. The four would have remanded the case to allow state regulators to prove that tobacco manufacturers had alternative "sufficient" means of communication of their advertising message. *See* Linda Greenhouse, *Justices Rein in Local Regulation of Tobacco Ads*, N.Y. TIMES, June 29, 2001, at A-1 (late edition). *See also* United States v. United Foods, Inc., 533 U.S. 405 (2001) (upholding mushroom growers' First Amendment free-speech right not to pay mandatory fees imposed on mushroom industry for advertisements of fresh mushrooms, fees assessed under a federal Department of Agriculture program approved in 1990 that authorized a one-penny per pound on mushroom producers, with Justices Stevens and Souter voting for the free-speech claim). *Compare* Glickman v. Wileman Bros., 521 U.S. 457 (1997) (holding against the free-speech claim of growers of certain fruits when the federal agricultural program covered marketing orders and advertisements, not merely advertisements, with Justices Stevens and Souter voting against the free-speech claim). *But see* Federal Elec. Comm'n v. Colorado Republican Fed. Campaign Comm., 533 U.S. 431 (2001) (upholding federal spending limits imposed on political advertisements made by state and national political parties as against the parties' claimed First Amendment free-speech rights, in line with post-Watergate Era precedent). Buckley v. Valeo, 424 U.S. 1 (1976) (upholding contribution limits imposed on political spending); *compare* Colorado Republicans v. Federal Election Commission, 518 U.S. 604 (1996) (finding unconstitutional the federal limits imposed on political parties' "independent expenditures"). The First Amendment right to advertise cigarettes and mushrooms is stronger, at least on a surface reading, than the First Amendment right to pay monies to political candidates. Just as the Court is clearly adopting a policy sympathetic to the national need to limit spending [by influence-peddlers] in political campaigns, the Court should recognize the national need to weigh personal data-privacy rights more heavily in the balance than an alleged First Amendment right of commercial interests to collect and disseminate personal data without consent of the data subject.

48. *Bigelow*, 421 U.S. 809.

effect on the national psyche.[49] Recently, again, in *Bartnicki v. Vopper*, the High Court has signaled the vulnerability of the individual's personal privacy rights to First Amendment rights of commercial free speech.[50] *In casu* a radio commentator's "First Amendment right" to broadcast a private cellular telephone conversation, which had been intercepted by a third party without knowledge or consent of the conversing parties, trumps any expectation of personal privacy rights, the Court's having noted circumstances implicating the public interest.[51] Adhering to its own

---

49. *See* SUT JHALLY, THE CODES OF ADVERTISING: FETISHISM AND THE POLITICAL ECONOMY OF MEANING IN THE CONSUMER SOCIETY (Routledge 1990); MICHAEL SCHUDSON, ADVERTISING, THE UNEASY PERSUASION: ITS DUBIOUS IMPACT ON AMERICAN SOCIETY (Basic Books 1986); KALLE LASN, CULTURE JAM: THE UNCOOLING OF AMERICA (Eagle Brook 1999).

50. Bartnicki v. Vopper, 532 U.S. 514 (2001) "Persons whose cellular telephone conversation had been intercepted and taped by unknown third party sued media defendants who broadcast tape and individual who had given tape to media, asserting claims under federal and Pennsylvania wiretapping acts. On interlocutory appeal, the Third Circuit Court of Appeals, 200 F.3d 109, found that application of statutes to defendants unduly infringed their free speech rights, and directed judgment for defendants. The Supreme Court, Stevens, J., held that: (1) wiretap acts' prohibitions against intentional disclosure of illegally intercepted communication which disclosing party knows or should know was illegally obtained are content-neutral laws of general applicability, and (2) application of those provisions against defendants violated their free speech rights, since tape concerned matter of public importance and defendants had played no part in the illegal interception. Affirmed. Justice Breyer filed concurring opinion joined by Justice O'Connor. The Chief Justice filed a dissenting opinion joined by Justices Scalia and Thomas." *Id.* (quoting Introductory Text from Westlaw).

51. *Id.* at 516. The circumstances *in casu* implicating the public interest were: "The first interest identified by the Government—removing an incentive for parties to intercept private conversations—does not justify applying § 2511(1)(c) to an otherwise innocent disclosure of public information. The normal method of deterring unlawful conduct is to punish the person engaging in it. It would be remarkable to hold that speech by a law-abiding possessor of information can be suppressed in order to deter conduct by a non-law-abiding third party. . . . There is no evidence that Congress thought that the prohibition against disclosures would deter illegal interceptions, and no evidence to support the assumption that the prohibition reduces the number of such interceptions. . . . The Government's second interest—minimizing the harm to persons whose conversations have been illegally intercepted—is considerably stronger. Privacy of communication is an important interest. However, in this suit, privacy concerns give way when balanced against the interest in publishing matters of public importance. One of the costs associated with participation in public affairs is an attendant loss of privacy. The profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide open supported this Court's holding in New York Times Co. v. Sullivan, 376 U.S. 254, 84 S. Ct. 710, 11 L. Ed.2d 686 (1964), that neither factual error nor defamatory content, nor a combination of the two, sufficed to remove the First Amendment shield from criticism of official conduct. Parallel reasoning requires the conclusion that a stranger's illegal conduct

Bigelow precedent, the majority of the Court seems to turn a deaf ear to the violated individual's interest in freedom from unwarranted intrusions of reasonable expectations of personal privacy. But, Chief Justice Rehnquist writes for the dissentients:

> Surely 'the interest in individual privacy,' *ante*, . . . at its narrowest must embrace the right to be free from surreptitious eavesdropping on, and involuntary broadcast of, our cellular telephone conversations. The Court [majority opinion] subordinates that right, not to the claims of those who themselves wish to speak, but to the claims of those who wish to publish the intercepted conversations of others. Congress' effort to balance the above claim to privacy against a marginal claim to speak freely is thereby set at naught.[52]

In another important opinion the Supreme Court has denied certiorari in *U.S. West, Inc. v. FCC*,[53] letting stand a federal Court of Appeals decision which questions the authority of the FTC to require opt-in procedures and to prohibit opt-out programs. An opt-in (by the consumer) is more onerous to business than the consumer opt-out procedure which requires the consumer to take affirmative steps to decline (opt out) having personal data collected, used, and disseminated. In obiter dictum, the Tenth Circuit Court of Appeals says the U.S. Congress has the power to regulate data privacy, including the invalidation of an opt-out procedure, under the Interstate Commerce Clause of the U.S. Constitution. And the Supreme Court has squarely upheld the power of Congress to regulate privacy to some extent under the Interstate Commerce Clause.[54]

The aforementioned sectoral approach to ensuring data privacy is further realized by such piecemeal legislation as the federal Identity Theft

---

does not suffice to remove the First Amendment shield from speech about a matter of public concern." *Id.* (quoting the Syllabus provided by the Reporter of Decisions).

52. *Bartnicki*, 532 U.S. at 555-56 (dissenting opinion).

53. U.S. West, Inc. v. F.C.C., 182 F. 3d 1224 (10th Cir. 1999), *cert. denied*, 530 U.S. 1213 (2000).

54. Reno v. Condon, 528 U.S. 141 (2000). (holding Driver's Privacy Protection Act of 1994, 18 U.S.C. §§ 2721-2725 (1994), prohibiting states' departments of motor vehicles from disclosing personal data about drivers, to be a constitutional exercise of Congress under Interstate Commerce Clause as against the Tenth Amendment state's interest, South Carolina's, in enacting a conflicting statute allowing ready sale to third party commercial interests of drivers' personal data). (Rehnquist, C.J., announcing in a unanimous opinion, "sale or release into the interstate stream of business is sufficient to support congressional regulation.") *Id.* (quoting Introductory Text from Westlaw) *Sed quaere:* regulation to what extent?

and Assumption Deterrence Act of 1998,[55] the Communications Decency Act of 1996, the Child On-line Protection Act of 1998 (COPA),[56] the Children's On-line Privacy Protection Act (COPPA) of 1998,[57] and the Electronic Signatures Act of 2000.[58] The sectoral approach is further exemplified by the FTC's attempts to encourage industry self-regulation[59] such as the adoption of data privacy codes of conduct and fair information practices, and the FTC's latter-day efforts at administrative governmental regulation.[60] In the pages which follow we briefly consider the mentioned laws in an attempt to present congressional efforts to address the thorny issue of data privacy.

1. Identity Theft Assumption and Deterrence Act

According to the FTC, between 500,000 and 700,000 victims annually report cases of identity theft in the U.S.[61] The Identity Theft Assumption and Deterrence Act ("Identity Theft Act"),[62] which is one of the more

---

55. Identity Theft Assumption and Deterrence Act, 18 U.S.C. §§ 1001(a) *et seq.* (2000) ("Identity Theft Act"). *See also* legislation amending Identity Theft Act, 18 U.S.C.A. § 1028 (2002).

56. Child On-line Protection Act of 1998, 47 U.S.C. § 231 (1998) [hereinafter COPA]. This Act is sometimes called CDA II since the Child Decency Act was held unconstitutional.

57. Children's On-line Privacy Protection Act, 15 U.S.C. §§ 6501 *et seq.* (2001) [hereinafter COPPA].

58. Electronic Signatures in Global and National Commerce Act of 2000, 44 U.S.C.A. § 3504 (2001). Each state is to pass implementing legislation concerning use of electronic signatures. Mark Ballard, *E-Sign: A Nudge, Not Revolution*, NAT'L L. J., Sept. 25, 2000, at B-1.

59. *See* Federal Trade Commission, *FTC 2000 Report to Congress, at* http://www.ftc.gov (last visited Aug.15, 2000). *Cf.* Federal Trade Commission, *Privacy On-line: A Report to Congress* (1999), *at* http://www.ftc.gov (last visited Aug. 15, 2000); and Federal Trade Commission, *Privacy On-line: A Report to Congress* (1998), *at* http://www.ftc.gov.

60. For example, the FTC filed its first enforcement action under the COPPA against Toysmart.com, Inc., an Internet toy retailer, by then in involuntary Chapter 11 Reorganization proceedings under the U.S. Bankruptcy Code. *See* text *infra* note 107. President Clinton signed into law on November 12, 1999, the Financial Services Modernization Act (Gramm-Leach -Bliley Act or GLB Act), 15 U.S.C. § 6801 *et. seq.* (1999) concerning financial institutions' practices. Per 15 U.S.C. § 6801 (§ 501 of GLB Act), financial institutions must respect customer privacy concerning "non-public personal information." The definition of "non-public personal information" is located at 15 U.S.C. § 6809(4) (§ 509(4) of GLB Act). The FTC's rules promulgated under the GLB Act are at 16 C.F.R. 313 (2002).

61. Stephen F. Laribee & Stephen D. Hogan, *Identify Theft: Will You Be the Next Victim?*, 46 NAT'L PUB. ACCT. 8 (2001).

62. 18 U.S.C. § 3663(a)(1)(B)(2) (2000) provides the legal definition of identity theft, a clear violation of personal privacy.

recent embodiments of the tentative, sectoral U.S. data-privacy model, is statutory recognition that technological advances have outpaced the U.S. legal system's ability to address the theft of an individual's identity.[63] Signed by President Clinton into national law on October 30, 1998, the Identity Theft Act criminalizes the unauthorized use of another person's identity (name and/or number) without authorization in order to engage in an activity which violates federal law (the law against identity fraud, for example) or activity that constitutes a felony under state or local law.[64]

Available data on U.S. identity fraud, while slim and of questionable quality, indicate ever-increasing occurrences.[65] In the past, identity thieves focused on physically stealing credit cards and other personal documents for their own criminal purposes. Today, it is much easier and less risky for computer-literate thieves to commit their identity-theft crimes over the telephone or Internet. One way they do so is by using what are called "card not present" transactions. In such instances thieves purchase items for delivery to their addresses by keying in identity numbers that belong to typically unaware individuals.[66] Another way is for the customer at the grocery store to swipe the credit card through the check-out machine without the cashier's looking at the card or verifying the user's identity.

E-tailers (electronic retailers) are particularly vulnerable to this credit-card fraud because it is they, not credit-card issuers, that must

---

63. The Identity Theft Act, spearheaded by Sen. John Kyl of Arizona, who acted as Chairman of the Senate Judiciary Subcommittee on Technology, Terrorism, and Government Information, passed the U.S. Senate unanimously.

64. Although many states recognize identity theft as a crime, the U.S. federalist system has resulted in a jumble of state laws dealing specifically with identity theft. *See, e.g.,* California, Cal. Penal Code § 530.5; Oklahoma, Okla. Stat. Tit. 21, § 1533.1; Tennessee, Tenn. Code Ann. § 39-14-150; Texas, Tex. Penal Code § 32.51. A summary of these laws is available at http://www.consumer.gov/idtheft/statelaw.htm (last visited Aug. 1, 2001).

65. Checking the FTC's Web site will reveal a precipitous rise in the reporting of identity theft. *See, e.g.,* Federal Trade Commission, *FTC Testifies: Identity Theft on the Rise, at* http://www.ftc.gov/opa/2000/03/ idtest.htm (last visited Apr. 17, 2002).

66. Social Security Numbers are especially valuable to identity thieves because those numbers serve as de facto national identifiers for virtually all Americans. *See Social Security: Use of the Social Security Number is Widespread: Hearing on Social Security Before House Comm. On Ways and* Means, 106th Cong. (2000) (statement of James G. Huse, Jr., Inspector Gen. of the Social Security Admin. Mr. Huse expresses the view that a Social Security Number in its incipience was never intended to act as a de facto national identity card and its growing use in electronic commerce has led to skyrocketing fraudulent misuses. He testifies that "the SSN has been transformed from a simple Agency record-keeping tool into a cornerstone of modern commerce. . . .*[It] was never intended to be a 'national identifier,' but over the years [it] became the 'de facto' identifier for Federal and State Governments.*" A law on Social Security numbers is pending before the 108th Congress (2001).

assume full responsibility for these financial transactions.[67] To compensate, many e-tailers confirm the validity of Internet credit-card orders by matching delivery information to cardholder addresses already on file; but sometimes e-tailers ship goods anyway, even if delivery address and cardholder address do not match. Indeed, many large, technologically sophisticated companies routinely garner Internet hits, with ensuing identity-fraud financial hits, by selling over the Internet items which, e.g., teenagers especially seem to like. This has resulted in a significant economic loss to their companies.[68]

The Identity Theft Act at last grants the victim of identity theft, formerly often ignored by law-enforcement officials, the right to demand prosecution of the perpetrators. Now this victim can sue for restitution, bringing suit before overt acts of common-law fraud are committed against financial institutions or even before documents are fraudulently manufactured. The crime under the Identity Theft Act is theft of the information itself (not merely the theft of personal documents) and reflects the unassailable fact that personal information has become all too readily available through the Internet.[69]

In granting *locus standi* to victims, the Act implicitly recognizes an individual's right to privacy regarding personal financial information, at

---

67. Cybercrime, which plagues "e-tailers", presents this privacy issue: When should the government be able to intrude into reading private data? On July 28, 2000, the Queen assented to the United Kingdom's Regulation of Investigatory Powers (RIP) Act, giving controversial powers to law-enforcement officials, including the right to intercept e-mail, subject to judicial scrutiny, and requiring businesses to supply decoding keys to the government for encrypted material. The RIP was enacted under Article 5.1 of the Council Directive 97/66/EC on EU Telecommunications Data, Article 5, 1998 O.J. (L 024) 1-8 which requires member states to ensure confidentiality of communications over public telecommunications systems. Part I of RIP makes it unlawful to intercept public and private telecom systems, as well as a tort for one running a private system to intercept that private system. *UK Passes Controversial E-Mail Interception Law*, EUROPEAN NEWSLETTER 1 (Croner-CCH, Issue 27, Aug. 2000). See the UK Department of Trade and Industry Web site regarding the business-practice regulations: http://www.dti.gov.uk/cii (last visited Apr. 15, 2002). It will be interesting to see if the EU court finds the UK in violation of the 1995 Data Privacy Directive. In Fall 2000, the Council of Europe proposed a convention to prevent cyber crime. Krotoszynski, *supra* note 35 (proposing that states legislate that no property interest exists in data comprising personal information so that the government which regulates data privacy will not be violating the Takings Clause of the U.S. Constitution).

68. Dennis Berman, *Card Sharps*, BUS. WEEK (Special Ed.), Apr. 3, 2000, at 68-76.

69. Mr. James Bauer of the U.S. Secret Service in testimony on May 20, 1999, before Sen. Kyl's Senate subcommittee, before enactment of the Identity Theft Act (quoted in Congressional Press Release, Press Release of Sen. Kyl, 'Identity Theft' Bill Passes Senate Unanimously, July 31, 1998, at 1.

least a right to privacy vis-à-vis a thief who appropriates an individual's financial identity. The fraud element of *scienter* is necessary in that the identity thief must act knowingly and willingly,[70] and the statement or misrepresentation made by the identity thief must be material.[71] In a departure from common-law fraud, the victim granted standing to sue under the Act is not the business identities defrauded, but the person whose financial identity has been misappropriated.[72]

With the Identity Theft Act, a private victim is now able to declare to law enforcement authorities that the perpetrator has committed a federal felony and should be punished under federal criminal law. The victim now has standing to seek restitution. Under prior law, only the merchant or financial institution was considered a direct victim of identity theft, but the consumer victim was considered an indirect victim, and thus denied standing to sue. The Act now not only mandates standing but also restitution to victims of certain crimes. The statute recompenses the victim for losses incurred, including attorney's fees and other expenses incurred in clearing one's name and credit rating. Furthermore, Congress requires the U.S. Sentencing Commission to consider identity fraud as a crime under the rubric of fraudulent crimes which are subject to the Sentencing Guidelines.

The Identity Theft Act, imposing stiff criminal penalties for violation,[73] directs the FTC to set up a complaint center and to maintain a database of identity-theft crimes and complaints. This clearinghouse is to acknowledge consumer complaints, refer them to law-enforcement authorities, and refer victims to the credit bureaus. The FTC must also maintain a telephone hotline for consumer victims of identity theft (currently at telephone number 1-877-438-4338).

Critics contend that the Identity Theft Act contains lacunae and is not adequately far-reaching.[74] As technology becomes more integrated, as data sources can be gathered from the Internet by clicking on one or two Web sites, the danger of abuse heightens and personal privacy will be proportionately more threatened. For example, personal information from court records on-line from North Dakota can now be retrieved by one click of a computer anywhere in the world. Typing the name of a data subject (e.g., John Doe) into a computer search engine on the Internet can retrieve vast

---

70. Identity Theft Act, 18 U.S.C. § 1001(a) (2001).

71. *Id.*

72. *See supra* note 67 and accompanying text.

73. Each violation carries a maximum of fifteen years in jail and/or a $250,000 fine, a period of three years of supervised release, and a special monetary assessment of $100.

74. Lisa Guernsey, *What Did You Do Before the War?*, N.Y. TIMES, Nov. 22, 2001, at G1.

amounts of identifying, personal information so that identity thieves can steal and assume that identity all the more readily.

2. Communications Decency Act of 1996

As enacted, the federal Communications Decency Act of 1996 (CDA)[75] had two purposes: (1) to protect children from indecency on the Internet, and (2) to foster growth of the Internet. Of particular interest were sections 223(d)(1)(A) and (d)(1)(B) of the CDA which made it a crime to display patently offensive messages or images to minors. In essence, the Act prevented Internet users from using the Internet to communicate material to minors which would be "patently offensive" to minors under "contemporary community standards."

Any attempt to regulate the content of free speech, even indecent speech that is not quite obscene, is highly suspect under the First Amendment. The American Civil Liberties Union brought a facial challenge to certain provisions of the Act, which made it a crime knowingly to send an obscene or indecent message or image to a person whom the sender knew to be under eighteen years of age.[76] The majority of the High Court found impermissible censorship in the Act:

> As a matter of constitutional tradition, in the absence of evidence to the contrary, we presume that governmental regulation of the content of speech is more likely to interfere with the free exchange of ideas than to encourage it. The interest in encouraging freedom of expression in a democratic society outweighs any theoretical but unproven benefit of censorship.

The Court made short shrift of the government's second contention that the Act fostered growth of the Internet. Despite the government's assertion of an equally significant interest in fostering the growth of the Internet, the Court said this second interest did not provide an independ-

---

75. The Communications Decency Act, 47 U.S.C. § 223(d) (1996) provided that: whoever "(1) in interstate or foreign communications knowingly (A) uses an interactive computer service to send a specific person or persons under 18 years of age, or (B) uses any interactive computer service to display in a manner available to a person under 18 years of age, any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs, regardless of whether the user of such service placed the call or initiated the communication; or (2) knowingly permits any telecommunications facility under such person's control to be used for an activity prohibited by paragraph (1) with the intent that it be used for such activity shall be fined under Title 18, or imprisoned not more than two years, or both.

76. 47 U.S.C. §§ 223(a)(1)(B) (1994, Supp. II).

ent basis for upholding the constitutionality of the CDA. Justice O'Connor disagreed, dissenting in part and concurring in part. She viewed the CDA as little more than an attempt by Congress to create "adult zones" on the Internet. The Court's own precedent, she argued, indicates that the creation of such zones can be constitutionally sound. Despite the soundness of its purpose, however, portions of the CDA are unconstitutional because they stray from the blueprint which prior cases have developed for constructing a zoning law that passes constitutional muster. O'Connor wrote:

> [Adult] zones can be constitutionally sound. Despite the soundness of its purpose, however, portions of the CDA are unconstitutional because they stray from the blueprint our prior cases have developed for constructing a "zoning law" that passes constitutional muster.... States have also denied minors access to speech deemed to be "harmful to minors." The Court has previously sustained such zoning laws, but only if they respect the First Amendment rights of adults and minors. That is to say, a zoning law is valid if (i) it does not unduly restrict adult access to the material; and (ii) minors have no First Amendment right to read or view the banned material. As applied to the Internet as it exists in 1997, the "display" provision and some applications of the "indecency transmission" and "specific person" provisions fail to adhere to the first of these limiting principles by restricting adults' access to protected materials in certain circumstances. Unlike the Court, however, I would invalidate the provisions only in those circumstances.[77]

The majority of the Court worried that a "community standards criterion" for Internet usage is unworkable because the Internet has a worldwide audience. This worldwide audience makes it likely that any offensive speech would be judged not by cosmopolitan standards but by the

---

77. Reno v. ACLU, 521 U.S. 844, 886-88 (1997) [hereinafter *Reno II*]. In a separate opinion, Justice O'Connor writes, "None of these provisions purports to keep indecent (or patently offensive) material away from adults, who have a First Amendment right to obtain this speech." *Id.* at 886. Sable Communications of Cal., Inc. v. Federal Communications Commission, et al., 492 U.S. 115 (1989) ("Sexual expression which is indecent but not obscene is protected by the First Amendment.") Thus, the undeniable purpose of the CDA is to segregate indecent material on the Internet into certain areas that minors cannot access. *See* S. Conf. Rep. No. 104-230, 189 (1996) (CDA imposes access restrictions . . . to protect minors from exposure to indecent material). "The creation of adult zones is by no means a novel concept. States have long denied minors access to certain establishments frequented by adults." (Justice O'Connor, with whom The Chief Justice joined, concurring in the judgment in part and dissenting in part).

standards of the community most likely to be offended by the objectionable Internet material.[78]

The Court found that the CDA violated the First Amendment, in part, for not defining its key terms, thus being unconstitutionally vague. And the majority of the Court viewed the statute as unprecedentedly overbroad. Most significantly for the current data-privacy issue, the Court said that the CDA was, e.g., not limited to commercial speech or commercial entities . . . [but rather] [i]ts open-ended prohibitions embrace all nonprofit entities and individuals posting indecent messages or displaying them on their own computers.[79]

Showing awareness of the different interests regarding commercial speech and noncommercial speech, the Court noted the affirmative defenses allowed by the Act would not be economically feasible for most noncommercial Web publishers.[80] Moreover, even for commercial publishers of Internet speech, the Court found no proof that technology could yet shield minors from harmful material.[81] Therefore, Congress had not tailored the Act narrowly enough to achieve the government's compelling state interest in protecting minors. Any statute attempting to regulate the content of speech must be precise and narrowly tailored.[82]

3. Child On-line Protection Act (COPA) of 1998[83]

Following hard on the successful challenge to CDA, the Child On-line Protection Act (COPA) tried to define key terms left unconstitutionally vague by the earlier Act and to cure the Act's other constitutional

---

78. *Reno II*, 521 U.S. at 877-78.

79. *Reno II* struck the CDA as unconstitutional. *See* ACLU v. Reno, 929 F. Supp. 824 (E.D. Pa.1996) [hereinafter *Reno I*] (addressing the CDA); ACLU v. Reno, 31 F. Supp 2d. 473 (E.D. Pa.1999) [hereinafter *Reno III*] (currently on appeal addressing the constitutionality of COPA); *see also* ACLU v. Reno, 217 F.3d 162 (3d Cir. 2000) (affirming district court's granting of preliminary injunction against application of COPA).

80. *Reno II*, 521 U.S. at 859-60 (finding the CDA unconstitutional as against the Free Speech Clause). According to the decision in *Reno II*, the CDA gave two affirmative defenses to prosecution: (1) that the minor used a credit card or some other age-verification system; and (2) that the user had made a good-faith effort to restrict the minor's access. *Id.* at 881-82.

81. *Id.* at 881.

82. *Id.* at 874. *See also* United States v. Playboy Entm't Group, Inc., 529 U.S. 803 (2000) (concerning the "bleeding" of offensive cable transmissions onto non-purchasers' television screens, occasioning the Court's saying, "Technology may one day provide another solution.").

83. COPA, 47 U.S.C. § 231 (1998). This Act is referred to as COPA and CDA II. *See* Catherine J. Ross, *Anything Goes: Examining the State's Interest in Protecting Children from Controversial Speech*, 53 VAND. L. REV. 427, 521 (2000).

defects.[84] COPA made it illegal for an individual or entity using the World Wide Web (but not the Internet as a whole)[85] in interstate or foreign commerce, knowingly and "with knowledge of the character of the material," to make "any communication for commercial purposes[86] that is available to any minor and that includes any material that is harmful to minors."[87] The phrase "harmful to minors" limits the scope of applicability of the Act. The Act sets out a tripartite test for whether published material is "harmful to minors," a test which the House Report on the proposed COPA expressly stated to be written so as to conform to the requirements of Supreme Court precedent.[88]

COPA is a further illustration of the piecemeal, ad hoc manner in which U.S. society has approached information privacy. Congress passed COPA in 1998 amid growing concern about children's access to sexually-explicit or indecent material over the Internet.[89] Presented as a legislative redress of the unconstitutional Communications Decency Act of 1996, COPA requires Web sites to filter out minors through good-faith defenses such as credit cards, debit accounts, adult identification codes purchased for the purpose, and other reasonable measures to verify users' ages.[90]

The theory under girding COPA may be extended to the issues of data transmission and data privacy. Congress is clear in its intent of addressing the pressing matter of the routine availability of obscene or indecent materials to children over the Internet. As a matter of public

---

84. H.R. REP. NO. 105-775, at 12 (1998); *See also* H.R. REP. NO. 105-225, at 2 (1998).

85. COPA defines "by means of the World Wide Web" as the "placement of material in a computer server-based file archive so that it is publicly accessible, over the Internet, using hypertext transfer protocol or any successor protocol." 47 U.S.C. § 231(e)(1) (1998).

86. COPA defines "commercial purposes" as "individuals or entities engaged in the business of making such communications." COPA defines a person engaged in the business as "one who makes a communication, or offers to make a communication, by means of the World Wide Web, that includes any material that is harmful to minors, devotes time, attention, or labor to such activities, as a regular course of such person's trade or business, with the objective of earning a profit as a result of such activities (although it is not necessary that the person make a profit or that the making or offering to make such communications be the person's sole or principal business or source of income.)" 47 U.S.C. § 231(e)(2)(B).

87. 47 U.S.C. § 231(a)(1) (1998).

88. The House Report regarding COPA aims to meet the Court's standards set out in Ginsberg v. New York, 390 U.S. 629 (1968), later modified by Miller v. California, 413 U.S. 15 (1973), in identifying patently offensive material. *See* H.R. REP. NO. 105-775, at 13 (1998).

89. 47 U.S.C. § 231 (1998). *See also* Children's On-line Privacy Protection Act, Pub. L. No. 105-277, 112 Stat. 2681, 15 U.S.C.A. §§ 6501 *et seq.* (1998) (also known as COPPA, defining a "child" as an individual under the age of thirteen).

90. 47 U.S.C. § 231(c)(1) (1998).

policy, this intent rings true with the American public at large. Likewise, the Identity Theft Act rings true, as both it and COPA represent attempts to preserve the privacy, however imperfectly defined, of a group society considers at risk.

The day after President Clinton signed COPA into law, the American Civil Liberties Union and others filed suit in federal court,[91] alleging that COPA: (1) violates the First Amendment because it infringes the free speech of adults and older minors, and (2) violates the Fifth Amendment because its language is unconstitutionally vague.[92] In *Reno III*,[93] the Federal Court of Appeals for the Third Circuit affirmed the U.S. District Court's grant of a preliminary injunction against enforcement of COPA. The court used the general standard for granting this extraordinary remedy: (1) the movant must show a reasonable likelihood of success on the merits of the case; (2) the movant shows irreparable harm resulting if the injunction is denied; (3) in balancing the interests of the parties, the movant's interests prevail; and (4) where the public interest is implicated, it is in the public interest to grant the relief.[94]

Viewing COPA as a content-based restriction on speech, the Court said the District Court correctly determined that COPA is "presumptively invalid and subject to strict scrutiny jurisprudence."[95] The Court of Appeals thought it likely that the challenged COPA statute would, on the merits, be found not narrowly enough tailored to meet a compelling state interest, and that COPA would not be the least restrictive means for protecting its interests considering the restriction placed on protected speech.[96]

If the courts apply to COPA the same standards they applied to the Communications Decency Act, then COPA, as an attempt to regulate the content of speech, even directed toward minors, may in fact be ruled unconstitutional.[97] Thus, in that event there will be further demonstration

---

91. *Reno III*, 31 F. Supp 2d. 473, 479 (E.D. Pa. 1999).

92. *Id.* (striking the CDA as unconstitutional). *See Reno I*, 929 F. Supp. 824, 849 (E.D. Pa. 1996) (addressing the CDA).

93. *Reno III*, 31 F. Supp 2d. at 498-99.

94. The *Reno III* federal court of appeals cited ACLU v. Black Horse Pike Regional Bd. of Educ., 84 F.3d 1471, 1477 n.2 (3d Cir. 1996) (en banc). ACLU v. Reno, 217 F.3d 162, 172 (3d Cir. 2000).

95. *ACLU*, 217 F.3d at 172 (citing *Reno III*).

96. *Id.*

97. Heather L. Miller, *Strike Two: An Analysis of the Child On-line Protection Act's Constitutional Failures*, 52 FED. COMM. L. J. 155 (Dec. 1, 1999). Prof. Miller detects four constitutional failures: (1) COPA's "harmful to minors" definition is not adaptable to the Internet because of the inherent difficulty of segregating adults from minors in cyberspace;

of the U.S.'s structural inability to come to grips with a privacy policy that is congruent with both the public interest and the Constitution. In this sense the contrast between the U.S. and the EU could not be more obvious.

The Third Circuit Court of Appeals invalidated COPA in June 2000, saying that one "cannot apply geographic standards to the Internet."[98] Is COPA constitutional in the view of the Supreme Court? *Ashcroft v. ACLU*[99] was argued in the October 2001 term of the Court.

4. The Unconstitutionality of the Child Pornography Prevention Act of 1996

Ashcroft v. The Free Speech Coalition 198 F.3d 1083 (2002),[100] one of the challenges to the Child Pornography Prevention Act of 1996 (CPPA), was decided in April 2002. The U.S. Supreme Court found that CPPA's ban on virtual child pornography was too broad to satisfy the Freedom of Speech guaranty. The speech prohibited by CPPA was "virtual" pornography, not child pornography leaving victims of a crime, and was not obscene. The Court's striking the CPPA as unconstitutional against the First Amendment stands as further demonstration of the U.S.'s structural inability to come to grips with a privacy policy that is congruent with both the public interest and the Constitution. As mentioned repeatedly here, in this sense the contract between the U.S. and the EU could not be more obvious.

5. Children's On-line Privacy Protection Act of 1998 (COPPA)[101]

---

(2) the vagueness of the "harmful to minors" language; (3) COPA's good-faith defenses are economically and technologically unavailable to many Web sites affected by the act, implying that Web site owners must provide material only to minors and not to adults who have a constitutional right to obtain material that would otherwise be available to them; and (4) Web sites will lose visitors because many adults will choose to safeguard their privacy by not inputting personal information required to access certain Web sites.

98. David L. Hudson, Jr., *Purient Protections, Prohibitions*, 87 A.B.A. J. 32 (Oct. 2001). *See also* DANIEL A. FARBER, THE FIRST AMENDMENT 10, 149 (Foundation Press 1998).

99. Ashcroft v. ACLU, 533 U.S. 973 (2001) (argued in the Oct. 2001 term; petitioner's brief filed July 27, 2001).

100. Ashcroft v. The Free Speech Coalition, 198 F. 3d 1083 (2002), asked whether computer-generated images of child pornography are entitled to First Amendment protection. The CPPA of 1996 attempted to bar sexually explicit material appearing to represent a minor child or convey the impression that minor children are depicted pornographically. *See also* New York v. Ferber, 458 U.S. 747 (1982) (upholding constitutionality of New York child pornography statute on rationale that child actors are necessarily harmed by engaging in pornographic representations).

101. Children's On-line Privacy Protection Act of 1998 ("COPPA"), Pub. L. No. 105-277, Div. C, Title XIII, 112 Stat. 2681-2728 (1998).

The focus of the Children's On-line Privacy Protection Act of 1998 (COPPA), as codified at 15 U.S.C. sections 6501-6506, is on privacy rights. Section 6502(a)(1) makes it unlawful

> for an operator of a Web site or on-line service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under [the regulations to be promulgated within a year from October 21, 1998].[102]

COPPA prohibits the disclosure of a child's personal data for any purpose, "except where such information is provided to a person other than the operator who provides support for the internal operations of the Web site and does not disclose or use that information for any other purpose. . . ."[103] A violation of these regulations is considered a violation of a rule defining an unfair or deceptive trade practice under the FTC Act.[104] COPPA differs from COPA primarily in how the latter attempts to regulate the content of speech to curb indecent or obscene speech.

The FTC filed its first two privacy-misrepresentation cases under COPPA, against GeoCities[105] and Liberty Financial,[106] thereafter reaching consent decrees in both. Then, the FTC filed its first successful COPPA enforcement action against the Internet company Toysmart.com. Facing forced bankruptcy, Toysmart.com wished to sell its single corporate asset, a customer database containing private personal information about its customers, in order to raise money for paying its creditors. Notwithstanding the bankruptcy court's permission to sell the database, the FTC action prevented the sale because the firm had promised its customers that their personal information would never be transferred to a third party.[107]

---

102. "Child" is defined in § 6501(1) as an individual under the age of thirteen. Section 6501(2) defines "operator" as an person operating a [*commercial*] Web site on the Internet or an on-line service and "who collects or maintains personal information from or about the users of or visitors to such Web site or on-line service," or agents of such an operator. The term "operator" includes persons offering products for sale in interstate or foreign commerce.

103. *Id.* § 1302(4), defining "disclosure."

104. The FTC Rule, Section 18(a)(1)(B) of the F.T.C. Act, 15 U.S.C. § 57(a)(1)(B) (1998).

105. FTC Docket No. C-3849 (Feb. 12, 1999).

106. FTC Case No. 9823522, filed under the Children's On-line Privacy Protection Act, Pub. L. No. 105-277, 112 Stat. 2681, 15 U.S.C. § 6501 (1998) ("COPPA").

107. Soon after Toysmart.com filed a petition in bankruptcy, it displayed a privacy seal as a licensee of TRUSTe, a company which certifies the privacy policies of on-line retailers by allowing use of its privacy seal. In a 3-2 decision, the FTC found that the firm violated its own privacy policy and the F.T.C. Act, 15 U.S.C. § 45(a) (1998), which prohibits deceptive

COPPA is inadequate to protect U.S. children on-line. For example, the child erroneously listing a birth date so as to appear over thirteen years of age will be allowed ready access to Web server portals.

6. Electronic Signatures ("E-sign") Act and Uniform Computer Information Transfer Act (UCITA)

Digital executions or e-signatures[108] have become the subject of U.S. national legislation. On June 30, 2000, President Clinton signed into law the Electronic Signatures in Global and National Commerce Act of 2000 (e-Signatures Act), becoming effective on October 1, 2000. This national legislation facilitates paperless business, allowing electronic authentication of contracts in digital form. It also necessarily raises e-commerce privacy concerns, but mostly will affect the ways in which businesses, not consumers, conduct business on-line.

This Act, which has legislative history stretching back at least three years,[109] requires users of documents signed digitally to agree to accept those electronically signed documents and to receive them over the Internet. It does not prescribe the technologies that must be used in verifying a digital signature, nor does it mandate a specific security protocol (such as iris scans or thumb print scans) for verifying the identity of the users. Thus, it leaves the choice among emerging new technologies and protocols to the marketplace itself. In this sense, the e-Signatures Act

---

acts of practices. FTC v. Toysmart.com, Inc., No. 00-11341-RGS, amended complaint filed and settlement announced (D. Mass., 2000). The bankruptcy court had declined to intervene in the matter, ruling that until there is a buyer for the customer list, the company can proceed with its proposed asset sale. See www.usatoday.com/life/cyber/tech/cti414. The FTC and Toysmart.com settled when Toysmart.com agreed to delete or de-personalize any information collected in violation of COPPA.

108. *See supra* notes 34 and 57 and accompanying text. With regard to the Electronic Signatures in Global and National Commerce Act, each state is to pass implementing legislation concerning use of electronic signatures. Ballard, *supra* note 58. The American Law Institute rejected the proposed new Article 2B to the Uniform Commercial Code, designed to cover sales of computer software and "smart" goods. The National Conference of Commissioners on Uniform State Laws (NCCUSL) then presented the same proposed statute to the states as the Uniform Computer Information Transactions Act (UCITA).

109. Rep. Eshoo, for example, introduced The Electronic Commerce Enhancement Act of 1997, which would require use of digital signatures for electronically submitting federal forms and assorted paperwork. It failed to leave committee, as did the Electronic Data Security Act of 1997, which was intended to assure users that the information they transmitted electronically, including their own signatures, would be safeguarded and held in great confidence. Other bills did not survive either, including the Computer Security Enhancement Act of 1997, the Electronic Financial Services Efficiency Act of 1997, the Digital Signature and Electronic Authentication Law of 1998 (both in the House and in the Senate), and the Government Paperwork Elimination Act of 1998.

runs parallel to EU Directive 1999/93/EC (December 1999) inasmuch as the EU directive leaves it to the member states to enact implementing national legislation comporting with the particular EU directive.

Some critics, mainly in Europe, see as a major flaw the absence of a specified protocol for verifying a signature.[110] Currently parties involved in high-value transactions, such as business contracts, require electronic signatures to be authenticated by digital certificates supplied, for a fee, by firms known in Britain as certificate authorities. These certificate authorities can be banks, investment banks, and international accounting firms like, among others.

Critics apparently question both the notion of authentication and the very legality of electronic signatures, wondering in the process if signatories to a transaction may compromise its integrity when they sign electronically, using procedures which have not been specifically recognized by authorities as safe and secure.[111] Indeed, it is not difficult to imagine electronic signatures being diverted or stolen, copied, and sold on an Internet black market in a fashion similar to stolen credit card numbers. As yet, though, acceptance of electronic signatures and usage of those signatures in electronic transmissions are too new to have identified conspicuous flaws in design or execution of transmission systems to warrant specific redress. To date only broadly-worded safeguards are in place.[112]

Regarding the Uniform Computer Information Transfer Act or UCITA, a uniform law on contracts offered to the states for adoption involves electronic data transfer in the new e-economy, covering the sale or lease of computer software and smart goods (containing computer information). This is part of the U.S. patchwork of state and federal laws, and is yet to be adopted by many states. After the American Law Institute (ALI) rejected, in 1999, the proposed Article 2B for addition to the

---

110. George Malim, Communications Week International, *E-Commerce: Users See Flaws in Electronic Signatures Act* (July 17, 2000), *available at* http://www.totaltele.com/CWI. On encryption and the ESA, George Malim wrote, "Digital certificates [authorization from Certification Authority] link the signatory's electronic identity to their [sic] physical identity using public key infrastructure (PKI), which has become the de facto encryption technology upon which high-value electronic transactions are based." *Id.*

111. *Id.*

112. The Commodity Futures Trading Commission, 65 Fed. Reg. 12466-12469 (Mar. 9, 2000), has accepted electronic signatures in lieu of handwritten signatures for users under its supervision. The Commission does require, though, that users, in its words, "must adopt and utilize reasonable safeguards regarding the use of electronic signatures, including at a minimum safeguards employed to prevent alteration of the electronic record with which the electronic signature is associated, after such record has been electronically signed." *Id.* at 12469.

Uniform Commercial Code to govern transactions in software and smart goods, the text was instead incorporated into the controversial Uniform Computer Information Transactions Act (UCITA), finalized in July 1999 and adopted by the National Conference of Commissioners on Uniform State Laws (NCCUSL).[113]

7. Various Privacy Statutes Pending Before the 108th United States Congress

A number of privacy statutes have been left pending before the 108th Congress, as before the 107th and 106th Congresses. Instead of lengthening this article beyond its elastic limits, we merely add a footnote referring to a Web site which summarizes the bills pending.[114]

B. U.S. Constitutional Issues

The 1995 EU Data Privacy Directive recognizes the tension that naturally exists between: (1) the right to privacy concerning personal data and (2) the right of freedom of speech, including the freedom of business to engage in commercial speech or commercial advertising. In the case of personal data, freedom of commercial speech as a First Amendment freedom would arguably include the freedom to disseminate data having left the hands of the data subject. Disallowing business the right to collect and disseminate personal data belonging to the data subject would cause business to argue the suffering of a "taking,"[115] oblivious to the initial unauthorized "taking" from the data subject of personal data to be used and transferred onward. U.S. law and business practice have so far given primacy to business' secondary "takings" argument over the individual's primary "takings" claim. It is this initial "taking" from the data subject that U.S. privacy law should protect. U.S. tort law has in an analogous sense recognized this initial privacy right by granting a tort cause of action for wrongful appropriation of personality or identity, in which one has a personal, proprietary interest.[116] Professor Ronald J. Krotoszynski proposes that the states enact legislation specifically stating that no

113. Scott J. Burnham, Symposium, *Perspectives on the Uniform Laws Revision Process*, 52 HASTINGS L.J. 603 (2001); Jean Braucher, Symposium, *Consumer Protection and the UCC*, 75 WASH. U. L.Q. 1 (1997). Article 2B was rejected by the ALI for the Uniform Commercial Code but proposed by the National Conference of Commissioners on Uniform State Laws to the states as a uniform law.

114. The Center for Democracy and Technology, *available at* http://www.cdt.org (last visited Nov. 4, 2001).

115. Professor Cate makes this argument. Cate, *supra* note 35.

116. RAY YASSER, ET AL., SPORTS LAW: CASES AND MATERIALS 767-80, 783-803 (4th ed. 2000).

property interest exists in personal data.[117] This would avert business' "takings" argument.

We profoundly disagree with those who read the First Amendment as barring an omnibus national data-privacy law in the U.S. Professor Fred Cates, for example, sees the balance of harm from such a statute to lie on business and not the individual:

> The U.S. approach to information privacy inevitably results in some harm to individuals' privacy, reputations, and sensibilities. But it represents a constitutional calculation that such harm is less threatening to the body politic than the harm associated with centralized privacy protection, government interference with the information flows necessary to sustain democracies and markets, and the growing ineffectiveness of omnibus legal controls in the face of the widespread proliferation of powerful information technologies. We should be loathe to alter that delicate constitutional balance lightly, by granting to the government new authority to interfere with the flow of information in the search for new–but often illusory and costly–protection for personal privacy.[118]

Only recently would any national overarching data-privacy statute be subject to serious attack as an unconstitutional violation of the First Amendment freedom of commercial speech[119] (and possibly as a violation of the Takings Clause).[120] For it was not until 1965 that the U.S. Supreme Court found that a federal statute violated the free speech guaranty of the First Amendment to the Constitution.[121] And it was only in 1975,[122] in

---

117. Krotoszynski, *supra* note 35.

118. Cate, *supra* note 35.

119. The same is probably true regarding the Takings Clause. The Fifth Amendment of the U.S. Constitution protects private property generally. *Sed quaere*: Do on-line gatherers and disseminators of personal data, often collected without the knowledge and/or consent of the data subject, have a "property interest" in these data? *See* Ronald J. Krotoszynski, *The Information Autobahn*, 33 IND. L. REV. 233 (1999) (suggesting that state statutes legislate that there is no property interest in personal data). We disagree with those who read the First Amendment as barring an omnibus national data-privacy law in the U.S. *See, e.g.*, Cate, *supra* note 35. Professor Ronald J. Krotoszynski, Jr., counters these arguments nicely at 33 IND. L. REV. 233 (1999).

120. Krotoszynski, *supra* note 35.

121. Lamont v. Postmaster General, 381 U.S. 301 (1965) (invalidating a federal statute as violative of the First Amendment Free Speech Clause). In fact, it was not until after the "War Between the States," that the U.S. Supreme Court applied the Fifth Amendment of the Bill of Rights as against the *federal* government to invalidate federal action. The first instances were Reichert v. Felps, 73 U.S. 160 (1868); Hepburn v. Griswold, 75 U.S. 603 (1870), overruled by Knox v. Lee, 79 U.S. 457 (1870); and Boyd v. United States, 116 U.S.

Bigelow, that the High Court held commercial speech to be speech protected by the First Amendment. Even at that late date, however, the Court did not grant advertising unqualified protection under the First Amendment. Rather, it created a new, restricted category, "commercial speech," over which the government retained the power to regulate in order to ensure that commercial speech was truthful and not misleading.[123] The Court assigned a lower value to commercial speech than to individual speech.

Thirty-three years before *Bigelow*, in *Valentine v. Chrestensen*, the Supreme Court had found commercial advertising unprotected by the First Amendment.[124] It is now some twenty-six years after *Bigelow*. In the face of deleterious effects on U.S. society from commercial speech, particularly if *commercial speech* embraces the right to intrude into the informational privacy of individuals, it is time to re-think the so-called freedom of *commercial speech.*

Professor Jack M. Balkin of Yale University has written that "freedom of speech" is the new "freedom of contract."[125] By this he means that "freedom of commercial speech" has become the rallying cry for business in the twenty-first century in the way "freedom of contract" was in the 1930s when business was nestling within *Lochner*[126] and resisting various governmental attempts at regulation amidst the Great Depression.[127] Now, business interests that gather personal data and seek to protect that information under the First Amendment pervert the idea of "commercial speech" which was designed to protect consumers.[128] These businesses would identify their interests as coextensive with the interests of consum-

---

616 (1886). These cases are collected in LAURENCE H. TRIBE, AMERICAN CONSTITUTIONAL LAW 9 n.9 (2000).

122. Bigelow v. Virginia, 421 U.S. 809 (1975) (holding unconstitutional a Virginia statute which made it illegal to advertise for abortions as an unconstitutional imposition on freedom of speech). Roe v. Wade 410 U.S. 113 (1973) had in certain cases already declared an aspect of the constitutional right of a privacy which a woman enjoys regarding her reproductive decisions.

123. Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748 (1976).

124. Valentine v. Chrestensen, 316 U.S. 52 (1942) (finding commercial advertising unprotected by First Amendment) (holding superseded by Bigelow v. Virginia, 421 U.S. 809 (1975)).

125. JACK M. BALKIN, CULTURAL SOFTWARE: A THEORY OF IDEOLOGY (1998); Tamara C. Piety, *Merchants of Discontent*, 25 SEATTLE U. L. REV. 377 (2001).

126. Lochner v. New York, 198 U.S. 45 (1905).

127. *Id.*

128. *See* note 122 and accompanying text.

ers, but if this were so, one could assume the consumer could curtail business' incursions into personal privacy.

To offer a coherent discussion of this tension between data privacy and commercial freedom of speech, we must briefly present the two-century development of the right of commercial free speech in the U.S. Then we consider the arguable right of informational or data privacy.

1. The Right to Speak Freely

The controversy in the U.S. about freedom of the press and the more generalized freedom of speech (including freedom of commercial speech or advertisement) is as old as the American colonies. In the 18th-century Age of Enlightenment, Blackstone maintained that the liberty of the British press consisted of mere prohibition of prior restraints (censorship) upon publication, but manifestly did not grant freedom from censure for criminal speech once published.[129] It is axiomatic to students of colonial U.S. history that, in defiance of both Blackstone's limited definition of freedom of speech and even the instructions of the colonial judge, in 1735, an early colonial New York jury engaged in jury nullification and acquitted printer John Peter Zenger of seditiously libeling New York's colonial governor.[130]

At the Plenipotentiary Convention of 1787, which was called for the purpose of amending what had turned out to be the impracticable Articles of Confederation, each state appeared with its constitution already containing a Bill of Rights which guaranteed common-law protections against certain government intrusions. These protections included freedom of speech and certain rights to privacy as from warrantless searches and quartering of government troops in peacetime. If participants at the Constitutional Convention did not consider the specific issue of data privacy, inconceivable to them in their epoch, they did fear tyranny from government and governmental invasions of their privacy. Indeed, even Alexander Hamilton feared tyranny from the proposed House of Representatives, the interests of which he viewed as too narrow to protect the liberties of the people.

---

129. *See* WILLIAM BLACKSTONE, COMMENTARIES (1769). In our view, freedom of speech includes *a fortiori* commercial freedom of speech, but the latter might not deserve "constitutional" protection.

130. NEW YORK WEEKLY JOURNAL, Aug. 18, 1735. John Peter Zenger's defense attorney was Andrew Hamilton of Philadelphia. "Not guilty" consequently stood as a defense against libel by the press. See the printer Zenger's note, NEW YORK WEEKLY JOURNAL 4, Aug. 11, 1735, "The Printer, now having got his liberty again, designs God willing to Finish and Publish the Charter of the City of New York next week."

Certain drafters of the U.S. Constitution worried that its readers might infer that the drafters had intended to allow the federal government to derogate from certain natural or fundamental rights.[131] And so it was understood, almost from the beginning, and reluctantly agreed by many, that immediately upon acceptance of the Constitution, the states would advance a Bill of Rights, in the form of ten amendments to the Constitution, expressly to recognize the existence of certain fundamental or natural rights vis-à-vis the federal government.

For example, the First Amendment allayed the fears of early republicans, concerned about governmental incursions, by stating that Congress shall make no laws abridging the freedom of speech or of the press.[132] And no rights have been more zealously guarded by the U.S. Supreme Court than the First Amendment grants,[133] although none of the fundamental or natural rights is absolute, for the law must always consider the rights of others when determining the boundaries of a fundamental or natural right.

Even as late as 1870, in the *Slaughter-House* cases, the Supreme Court refused to hold that the Fourteenth Amendment's substantive due process guarantee applied to protect citizens of a particular state from certain "unconstitutional" state actions.[134] Until the post-Civil War paradigm shift, people understood that their particular state, as the fundamental expression of popular sovereignty, served as the cushion protecting them from intrusions by the federal government.[135] After the Civil War, though, the weight of concern seemed to shift to fear of intrusions by state governments. Treading cautiously, the High Court slowly interpreted the Fourteenth Amendment to have incorporated the Bill of Rights, thereby making Bill of Rights' guarantees applicable against state action, as well as against federal government action.[136]

---

131. EDMUND S. MORGAN, THE BIRTH OF THE REPUBLIC 131 (1963).

132. U.S. CONST. amend. I.

133. *See, e.g.*, Schaefer v. United States, 251 U.S. 466 (1920) (finding First Amendment freedoms so crucial to liberty that a republican instinctively recoils from any limitation placed thereon).

134. Slaughter-House Cases, 83 U.S. 36 (1873). Subsequently, the Court slowly began to read the Fourteenth Amendment as a protection against state action. *See, e.g.*, Lochner v. New York, 198 U.S. 45 (1905).

135. To illustrate this paradigm shift, it was not until after the Civil War that "the United States" became a singular noun requiring a single verb. Before the Civil War, the United States of America "were" (not "was") the government of limited powers.

136. *See generally* LAURENCE H. TRIBE, 1 AMERICAN CONSTITUTIONAL LAW 1293-1310 (2000). The U.S. Supreme Court has held in a series of cases that the fundamental rights, which the Bill of Rights guarantees from encroachments by the *federal* government, are protected from erosion by the *states*, i.e., from "state action," on the theory that the post-Civil War Fourteenth Amendment applies the Bill of Rights so as to limit actions taken by

A free people in a free government, the Founders thought, must have the right to praise or condemn their government, this right being the hallmark of a non-totalitarian state. In the free marketplace of ideas, of diverse knowledge and discussion between antagonists, the rationale goes, the truth will out.[137] In general, the government can protect an individual's right to privacy only by imposing reasonable time, place, and manner regulations upon free speech, and those regulations must be applicable to all speech regardless of its content. The government cannot foreclose conversation solely to protect the right of an individual to the privacy of not hearing the conversation, but only upon a showing by the government that substantial privacy interests are being invaded in an intolerable matter.[138]

But what of the dissemination of personal data having commercial value? Just as businesses do not share the same right of privacy as individuals, although corporations do retain some Fourth Amendment rights against unreasonable search and seizure, commercial interests do not enjoy the same right to freedom of expression as individuals do.[139]

Since the New Deal and its post-*Lochner* series of Supreme Court cases, the scope of permissible federal regulation of business has been extended to almost every commercial and farming activity.[140] Now, it is

---

the states. This line of cases represents a sharp departure from Barron v. Baltimore, 32 U.S. (7 Pet.) 243 (1833) which held, pre-Civil War, that if Congress had intended to apply the first eight amendments to the states (that is, to "state action"), Congress would expressly have done so. Recall, however, that James Madison's visionary line of thinking (as the principal drafter of the Edmund Randolph proposals which, with one exception, were accepted as the new Constitution in 1787), that the people of the various *states* needed protection from a Bill of Rights directed against tyrannical *state action* (as well as against federal action), was accepted in 1879 by the U.S. House of Representatives but not by the U.S. Senate. It took 89 years to vivify Madison's proposal, by congressional enactment of the Fourteenth Amendment in 1868, even though the U.S. Supreme Court moved at a glacial pace to find that the Fourteenth Amendment "incorporated" the provisions of the Bill of Rights so as to apply them against actions of the various states. *Id.*

137. *See, e.g.*, Thornhill v. Alabama, 310 U.S. 88; Gertz v. Robert Welch, Inc., 418 U.S. 323 (1974). In other words, the First Amendment demands freedom of political expression.

138. Erznoznik v. Jacksonville, 422 U.S. 205 (1975).

139. Valentine v. Chrestensen, 316 U.S. 52 (1942) (finding commercial advertising unprotected by First Amendment) (holding superseded).

140. Lochner v. New York, 198 U.S. 45 (1905). The *Lochner* era, with its laissez-faire approach to capitalism trumpeting the sanctity of "freedom of contract," held unconstitutional many attempts at governmental regulation of U.S. economic and social life, as violative of Substantive Due Process guaranties in the Constitution. The passing of the *Lochner* era roughly accompanied the Great Depression. Bruce Ackerman, *Constitutional Politics/Constitutional Law*, 99 YALE L.J. 453 (1989) discusses the remarkable expansion given the federal government by the Supreme Court, which began to uphold much of the

beyond cavil that the federal government is free to regulate economic activity in almost any way.[141]

As mentioned, until recently in the U.S., commercial interests in the main did not presume to invoke the First Amendment guaranty of freedom of speech as covering *commercial* speech. In *Valentine v. Chrestensen*, the Court allowed a city to ban commercial advertisements. In this decision, now overturned, the Court first agreed not to sidestep the issue of whether the First Amendment protected advertising and "commercial speech."[142] The Court held that commercial speech (left undefined) was not entitled to First Amendment protection, unlike *noncommercial* speech, which was within the protection of the First Amendment. The leafleteer's effort *in casu* to prevent New York City's regulation of his advertising was unsuccessful because, the Court said, even under the First Amendment government had the virtually untrammeled right to regulate commercial speech.[143] Then, in 1951, the Court held in *Breard v. Alexandria*,[144] that a door-to-door salesperson's commercial speech and movements were not protected by the First Amendment.[145]

Pittsburgh Press Co. v. Pittsburgh Comm. on Human Relations also involves freedom of commercial speech.[146] The opinion shows increasing Supreme Court reluctance to rely upon the *Chrestensen* precedent. Before enactment of the Civil Rights Act of 1964,[147] newspapers regularly

---

New Deal legislation, e.g., NLRB v. Jones & Laughlin Steel Co., 301 U.S. 1 (1937) (upholding constitutionality of the National Labor Relations Act of 1935, the "Wagner Act").

141. *See* TRIBE, *supra* note 136. See also, e.g., the Civil Rights cases finding constitutional the applicability of the Civil Rights Act of 1964 to almost every economic activity under the Commerce Clause of the Constitution.

142. Valentine v. Chrestensen, 316 U.S. 52 (1942).

143. *Id.*

144. Breard v. Alexandria, 341 U.S. 622 (1951).

145. *Id.*

146. Pittsburgh Press Co. v. Pittsburgh Comm. on Human Relations, 413 U.S. 376 (1973) (decided the same year as Roe v. Wade on abortion rights). In this case, the Supreme Court analogized the newspaper's gender-specific advertising practices to placing "a want ad proposing a sale of narcotics or soliciting prostitutes." In other words, the newspaper's advertising practice had by then become illegal under Title VII of the Civil Rights Act of 1964. *But see* the comment of DANIEL A. FARBER, THE FIRST AMENDMENT 10, 150 (1998): "The Court's analogy was not especially helpful; the narcotics ad is prohibited as the prelude to other illegal conduct by the advertiser, whereas the basis for prohibiting gender designation in want ads is that the ads *themselves* cause harm without any further action by the advertiser."

147. Title VII of the Civil Rights Act of 1964, 42 U.S.C.A. § 157 (1964), prohibited discrimination on the basis of race, sex, creed, national origin, or religion. This Act created the Equal Employment Opportunity Commission (EEOC).

advertised employment vacancies by gender. "Jobs for women" were distinctly advertised from "jobs for men." When the Pittsburgh Commission on Human Relations got its injunction from the court of first instance against such gender-designated advertisements, the Court upheld the injunction, but with a less than clear *ratio decidendi*.

The sea-change in U.S. jurisprudence came in 1975 in *Bigelow*.[148] A Virginia statute made it illegal to advertise for abortions, at a time just before the Supreme Court was to find in *Roe v. Wade*[149] a woman's *constitutional* right to seek an abortion, as part of her right to privacy as a fundamental human freedom. In *Bigelow*, when a Virginia newspaper published an advertisement for a New York abortion-referral service, it was easy to see governmental prohibition of the advertisement as an impingement upon a woman's constitutional right to travel from one state to another, separate and apart from the First Amendment commercial speech issue. Although *Bigelow* did not turn on the right to travel, in effect the federal right to travel trumped the interest of the State of Virginia in regulating commercial speech (advertising). The Court's language foreshadowed frank adoption of the principle that "commercial free speech" is *ipso facto* protected by the First Amendment.[150]

The Court, we urge, got it wrong in the next term's pertinent case, *Virginia State Bd. of Pharmacy*, in stating its intent to extend *Bigelow* to protect commercial speech which was not even designed to disseminate information in protection of a fundamental right (say, the right to reproductive privacy). The Court would better serve society by someday

---

148. Bigelow v. Virginia, 421 U.S. 809 (1975).

149. Roe v. Wade, 410 U.S. 113, *reh'g denied,* 410 U.S. 959 (1973) (upholding a woman's fundamental right of privacy in deciding to have an abortion).

150. Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748 (1976), was decided in the Court's next term, after *Bigelow*. A parallel case recently arose from the European Union involving an Irish woman's right to travel to England to obtain an abortion, in which the European Court of Justice managed to sidestep the issue of whether or not a woman in the EU has an overarching "supranational" right to obtain an abortion. Interestingly, essentially the same facts have plagued the European Union, where the Irish Republic remains overwhelmingly Roman Catholic and opposed to abortion rights. Society for the Protection of Unborn Children Ir. Ltd. v. Grogan, [1991] 3 C.M.L.R. 849 (Ir. S.C.) (provision of Irish constitution protecting right to life of unborn children and prohibiting abortions, arguably prohibiting publication of student handbooks listing abortion clinics legal in England, pitted against EU freedom to travel within the Community to obtain services). Attorney General v. X, [1992] 1 I.R. 1 (Ir. S.C.). (Irish court deciding not to issue order in the nature of a writ of *ne exeat* to prevent pregnant fourteen-year-old from traveling to England to obtain abortion, not on EU law principles but on Irish law's allowance of abortion when real and substantial risk to mother's life exists fear existed of girl's possible suicide).

soon recognizing the primacy of the public interest in setting outer limits on commercial speech, and re-reading *Bigelow* as necessitated only by the need greater than for "freedom of commercial speech." Society's greater need is to protect the right to privacy of a person seeking control over reproductive decisions which could not be attained in the absence of freely dispensed information.

The Court answered the question of what *Bigelow* really meant in *Virginia State Bd. of Pharmacy*.[151] The *Virginia State Bd. of Pharmacy* case came during the same period of judicial activism that resulted in *Roe v. Wade's* extremely controversial declaration that a woman has a fundamental right to privacy regarding her own procreative decisions. Until that time, the State of Virginia prohibited pharmacies from publicizing the prices of prescription drugs on the rationale that child-like consumers would flock to the pharmacy offering the lowest prices notwithstanding poor services. This case is a landmark for the proposition that the First Amendment accords advertising as commercial speech some degree of constitutional protection.

After *Bigelow* and before *Virginia State Bd. of Pharmacy*, no one was certain whether the Court really meant what it said about commercial free speech or, rather, intended to qualify the language by appending the right of commercial free speech to a more fundamental constitutional right such as the right of privacy. The Court in *Virginia State Bd. of Pharmacy* held: "It is precisely this kind of choice, between the dangers of suppressing information, and the dangers of its misuse if it is freely available, that the First Amendment makes for us."[152] Today, obvious parallels exist to personal-data privacy; the public need for allowing comparison shopping of necessary pharmaceuticals was properly weighed in the balance.

In *Bolger v. Youngs Drug Products Corp.*, the Supreme Court found that mailing unsolicited pamphlets, which advertised contraceptives prohibited by federal law, did constitute commercial speech. The Court decided for certain only that commercial speech in this case included advertisements which described a product, directly proposed a commercial transaction (sale of contraceptives), and were economically motivated on the part of the advertiser.[153] As in *Bigelow*, this case upholding freedom to disseminate commercial information implicated the right to make private procreative decisions.

Then, in 1980, in *Central Hudson Gas & Electric Corp. v. Public Service Comm.*, the High Court gave us our four-pronged definition of

151. *Virginia State Bd. of Pharmacy*, 425 U.S. 748.

152. *Id.*

153. Bolger v. Young Drug Products Corp., 463 U.S. 60 (1983).

"commercial speech" that is still employed today. This time the Court strayed from restricting its "right to advertise information" to prohibitions which would inform reproductive decisions. The Court struck a utility commission's ban on the advertising of utility rates as an overbroad regulation of commercial speech.[154]

Of course, this First Amendment right to commercial free speech is not absolute. For many years the FTC has had jurisdiction to regulate unfair or deceptive trade practices, including untruthful advertising (commercial speech).[155] And, as mentioned, in *Virginia State Bd. of Pharmacy*, the Supreme Court has held that the state could regulate deceptive or misleading commercial speech. The *Virginia State Bd. of Pharmacy* case has made it clear that the *Bigelow* court meant to extend the new "commercial speech doctrine" to cases in which the right of privacy was not implicated in the ways privacy had been jeopardized in *Roe v. Wade* and *Bigelow*.

And so now, under the *Central Hudson* test, to be protected by the First Amendment, the commercial expression must be commercial speech which is "truthful." Then the Court must ask, when the government is attempting to regulate this protected commercial speech, whether the government's interest in regulation is *substantial*. If the government interest is substantial, such as for consumer protection, the regulation must be pointed directly toward advancing that governmental interest, and the regulation cannot be *overbroad* for the task (compare the European Doctrine of Proportionality discussed *infra* Part V.A, which requires that the regulation in question adversely affect its targets no more than is "strictly necessary" for attaining the purpose for which the statute was enacted). The government seeking to regulate does not have to show a *compelling* state interest to regulate the commercial speech, rather only a *substantial* interest.[156] In summary, *Central Hudson* gives the current, controlling four-pronged test for commercial speech mentioned above.[157]

---

154. Central Hudson Gas & Electric Corp. v. Public Service Comm., 447 U.S. 557 (1980). If there is truthful commercial speech, and if the government interest in regulation of it is substantial, then, the Court said, "we must determine whether the regulation directly advances the governmental interest asserted, and whether it is not more extensive than is necessary to serve that interest." *Id.* at 566.

155. Federal Trade Commission Act, 15 U.S.C.A. § 41 (1914); *see supra* note 11 and accompanying text.

156. DANIEL A. FARBER, THE FIRST AMENDMENT 158-60 (1998) (discussing the boundaries of commercial speech).

157. *Central Hudson Gas & Electric Corp.*, 447 U.S. 557.

Now, with the meandering inexorability of precedential pollution, under the authority of *Bates v. State Bar of Arizona*,[158] *Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc.*,[159] and *Central Hudson*,[160] commercial advertising is within the protection of the First Amendment, although commercial speech is accorded a kind of second-tier protection, as it clearly may be subject to more regulation than may political or social speech.[161] *Bates*, *Bigelow*, and *New York Times Co. v. Sullivan* all make clear that commercial speech is not removed from protection of the First Amendment merely because the speaker's motive is primarily *economic*. This recent interpretation is an unfortunate late-twentieth-century gloss on the First Amendment to the Constitution. The right to informational privacy—the privacy of one's own data that constitute one's financial and personal identity—should get primacy of judicial consideration over the newly-created right of commercial free speech.

2. The Penumbral (Shadowy) Right to Privacy

In *Chase Sec. Corp. v. Donaldson*,[162] the Supreme Court referred to fundamental rights, such as those guaranteed in the Bill of Rights, as what used to be called natural rights of the individual. Although it is difficult to identify with certitude which are natural rights under natural law and which are not, generally U.S. law considers the right to privacy a natural right of the individual. Unlike the individual person, the corporate person generally does not enjoy a right to privacy, although of course the Fourth Amendment prohibition against unreasonable search and seizure applies to protect the corporation.[163] For instance, in *Bellis v. United States*,[164] a

158. Bates v. State Bar of Arizona, 433 U.S. 350 (1977).

159. Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748 (1976).

160. *Central Hudson Gas & Electric Corp.*, 447 U.S. 557.

161. These three cases all make clear that commercial speech is not removed from protection of the First Amendment: Bates v. State Bar of Arizona, 433 U.S. 350 (1977); Bigelow v. Virginia, 421 U.S. 809 (1975) (affording First Amendment protection to commercial advertising in a newspaper); and New York Times Co. v. Sullivan, 376 U.S. 254 (1964). Furthermore, they show that commercial speech is not removed from protection of the First Amendment merely because the speaker's motive is primarily economic. The First Amendment guaranty is not absolute, however. In *Virginia State Bd. of Pharmacy, Inc.*, 425 U.S. 748, the Supreme Court held that the state could regulate deceptive or misleading commercial speech.

162. Chase Sec. Corp. v. Donaldson, 325 U.S. 304, 314 (1945).

163. In *Joint Anti-Fascist Refugee Comm. v. McGrath*, 341 U.S. 123 (1951), the Court allowed standing to sue to plaintiffs, in a suit brought against the U.S. Attorney General, by those named on the Attorney General's list of members of Communist organizations.

business entity was found to enjoy no substantial claim of privacy regarding its financial records.

The Supreme Court has held that enumeration of certain guaranties in the U.S. Constitution creates penumbras, or shadows, from specifically guaranteed rights for certain fundamental rights, including the right to privacy.[165] This right to personal privacy vis-à-vis the government exists in the penumbra of the following enumerated rights:

- the right of privacy from governmental intrusion exists in the penumbra of the First Amendment's guaranties of freedom of speech and of the press, and of freedom of association;
- in the Third Amendment's prohibition on the peacetime quartering of troops in private homes;
- in the Fourth Amendment's prohibition on unreasonable searches and seizures;
- in the Fifth Amendment's guaranty against compelled self-incrimination;
- in the Ninth Amendment's reservation to the people of rights not specifically enumerated in the Constitution;
- and perhaps in the liberty which the Fourteenth Amendment's Due Process of Laws Clause protects.[166]

To illustrate, in *Griswold v. Connecticut*, the Supreme Court found that a married couple had a fundamental right of privacy which protects them from state interference in their use of contraceptives. The Court struck down as an unconstitutional intrusion on the couple's right of privacy a state statute which prohibited their use of contraceptives, not because the statute attempted to regulate sexual activity but because it sought to interfere with the intimate, private relationship of wife and husband.[167]

(Justice Jackson stated that the right of privacy is inapplicable to commercial organizations or corporations chartered by the state).

164. Bellis v. United States, 417 U.S. 85 (1974).

165. A seminal work on privacy in the United States contains Brandeis' dictum that privacy is the "Right To Be Let Alone." Samuel D. Warren & Louis D. Brandeis, *The Right of Privacy*, 4 HARV. L. REV. 193 (1890).

166. *See* the U.S. Constitution and Bill of Rights, as noted in text.

167. Concerning the right of privacy in the U.S. regarding the raising of a family, *see* Griswold v. Connecticut, 381 U.S. 478, 485-86 (1965).

Then, in *Roe v. Wade*, the Court recognized the penumbral right of privacy of a woman regarding her child-bearing decisions, holding that the Constitution granted her the right to have an abortion in the first trimester of pregnancy. The Court wrote that this right to privacy against governmental intrusion is not absolute, so the *Roe* plaintiff lost her right to privacy at the undefined moment the child's right to life and the state's interest therein became choate.[168]

The Court in *Madsen v. Women's Health Ctr.*[169] did not enunciate for U.S. non-criminal law a general principle of proportionality,[170] but came very close. In requiring that the "buffer zone" between the abortion-protesters and the abortion clinic be sharply tailored to be no larger than necessary to achieve the right to privacy, the Court mimicked "proportionality" jurisprudence from the EU Court of Justice, such as the *Bela Mühle* skimmed milk case discussed *infra* Part V.A.

Hill v. Colorado is a critical case for data-privacy rights, even though it is on the surface the Supreme Court's most recent abortion-rights decision.[171] We read this decision as foreshadowing the Court's willingness to uphold a comprehensive national data-privacy statute enacted by the Congress. *In casu*, full-blown free speech First Amendment rights (the rights of individual, noncommercial protest and expression), which are more zealously guarded than the lesser-valued right to freedom of commercial speech, were pitted against the fundamental human right of privacy. On the facts of *Hill*, the right of privacy took primacy since the Court upheld the state's police power to regulate the health, safety, and welfare of its citizens (by requiring a buffer zone), and by extension to the protection of the citizenry's right to privacy.

First, the Court balanced the interests at stake, acknowledging that each side presented "legitimate and important concerns" and labeling the First Amendment interests "clear and undisputed."[172] Recognizing that the right of free speech in the abortion-rights context is "substantial," the

168. Roe v. Wade, 410 U.S. 113, *reh'g. denied,* 410 U.S. 959 (1973) (concerning a woman's fundamental right of privacy in deciding to have an abortion).

169. Madsen v. Women's Health Ctr., 512 U.S. 753 (1994).

170. The Court has adopted a Proportionality Test for criminal law in *Terry v. Ohio,* a decision allowing a narrow exception for police officers to search individuals in a non-custodial situation—a balance must be struck allowing a reasonable search for protection of the police officer (a frisk). In other words, the Court adopted a balance between the Fourth Amendment intrusion and the government's interest in safety. *See* United States v. Bajakajian, 524 U.S. 321 (1998) (applying a kind of proportionality test to a criminal forfeiture case).

171. Hill v. Colorado, 530 U.S. 703 (2000).

172. *Id.* at 714.

Court determined that "the right of every person to be let alone must be placed in the scales with the right of others to communicate."[173] Clearly, this "right to be let alone"[174] is comparable although not identical to the present issue: the right of the on-line user to be let alone by commercial interests which would gather and disseminate her personal data.

In *Hill*, Justice Stevens wrote for the majority: "The question is whether the First Amendment rights of the speaker are abridged by the protection the [Colorado state] statute provides for the unwilling listener."[175] Privacy has special force in the privacy of one's home and its immediate surroundings but may even be protected, vis-à-vis the First Amendment right, in such confrontational settings as abortion protests held at a reproductive-rights clinic.

The particular state statute, under attack for impermissibly regulating free speech, prohibited protesters from coming within eight feet of a person seeking to enter a health facility. This restriction on First Amendment rights, incorporated by the Fourteenth Amendment to protect citizens against actions of the state, was constitutional, the Court said. The state statute was a narrowly-tailored content-neutral regulation of the time, place, and manner of the protesters' exercising their First Amendment Free Speech.[176] The Colorado statute did not impose prior restraint on freedom of speech, nor did it have a "different impact on conduct of some speakers" from its impact on others and, thus, was not constitutionally overbroad. Neither did the statute ban any form of communication, but was instead a content-neutral regulation of places where those communications could occur.[177]

In upholding the state's police power to regulate the health, safety, and welfare of its citizens,[178] as well as their right to privacy, the Court seems to blend the one with the other. The "health, safety, and welfare"

---

173. *Id.* at 726.

174. Warren & Brandeis, *supra* note 165. Surely, had they been prescient, their "right to be let alone" would have included the right to be free from commercial use of their personal data, as well as unsolicited and unconsented-to computer "cookies" and "Web bugs."

175. *Hill*, 530 U.S. at 708.

176. *Id.* at 719.

177. The federal district judge dismissed the protestors' complaint, holding that the statute imposed content-neutral time, place, and manner restrictions narrowly tailored to serve a significant government interest under *Ward v. Rock Against Racism*, 491 U.S. 781 (1989), in that Colorado had not "adopted a regulation of speech because of disagreement with the message it conveys." *Id.* at 719.

178. What the EU calls the member state's "safeguard clause" allowing the state or municipality to retain regulatory privileges at the expense of higher federal governing unit.

interest subsumes the "right to privacy" interest. The statute did make it more difficult, however, for the speakers to give unwanted advice to persons seeking to enter or leave the facilities.

We can easily apply the principles decided in *Hill* to the data-privacy issue. This *ratio decidendi* indicates that the same Court would probably find that the federal government, though cautioned by the Bill of Rights, could validate omnibus data-privacy legislation as a proper exercise of police power in order to protect the right to privacy of the data subject. It does not matter if the statute is a state statute or a federal statute because the right to be free from unwanted information usage by others could be vindicated by either state or federal power to regulate the health, safety, and welfare of the polity.[179] If *Hill* does indeed foreshadow the Supreme Court's inclination to uphold as constitutional an overarching national statute protecting the privacy of personal data, such a statute would suffice, at least under the current court.

The *Hill* Court said, "[O]ur cases have repeatedly recognized the interests of unwilling listeners in situations where 'the degree of captivity makes it impractical for the unwilling viewer or auditor to avoid exposure.'"[180] Similarly, on-line users are in a sense captive to companies making data profiles through, for example, computer applets and cookies, without the users' knowledge or consent. On-line users may also be captive to other methods used for unsolicited capture of personal data such as private medical information, communications indicating sexual preferences, or consumer proclivities from on-line purchases.

As long as on-line users may be considered captive in the same way persons seeking access to abortion clinics are captives, so too should on-line users enjoy the same opportunity "to avoid exposure."[181] This means

---

179. U.S. CONST. art. V.

180. *Hill*, 530 U.S. at 718. The Court cites Lehman v. Shaker Heights, 418 U.S. 298 (1974), and Erznoznik v. City of Jacksonville, 422 U.S. at 209.

181. The language of on-line data acquisition embraces such arcane items as *applets, cookies, Web bugs, spam, anonymizers*, and so forth. These and others relate directly to accessing, tracking, collecting, and/or hiding private on-line data. *See* Adam Cohen, *Internet Insecurity: The Identity Thieves are Out There and Someone Could Be Spying on You: Why Your Privacy on the Net is at Risk and What You Can Do*, TIME, July 2, 2001, at 45, 50. *See also* http://www.bugnosis.com; http://www.anonymizer.com; and http://www.cookiecentral.com. *See also* John Schwartz, *Tracks in Cyberspace: Government is Wary of Tackling Concerns about Privacy On-line*, N.Y. TIMES, Sept. 6, 2001, at A-1, C-1 (last of three articles). "Washington is not creating new laws and regulations that might restrict the use of cookies and other high-technology tools by businesses to monitor Internet users' activities. Some lawmakers say that the politics of privacy is so sensitive and complex that a deliberate approach is best–but there is a growing agreement that some kind of government action will eventually have to emerge."

that if an on-line user does not have the option to refuse to have personal data gathered and disseminated, "captivity" is more likely to be found than not. Yet, if the state enacted a statute prohibiting commercial interests from requesting to gather and use on-line personal data, such a statute would probably be overbroad, unnecessarily restrictive, and not sufficiently narrowly tailored to withstand judicial scrutiny. Viewed from either perspective, a regulatory statute must offer certain rights to both communicants on on-line communications. A commercial provider would have the right to offer to gather and disseminate personal information about a private person, but with that person's full knowledge and consent, just as that same person would have the right to refuse use or wider transmittal of that information.

The *Hill* Court stated, "The recognizable privacy interest in avoiding unwanted communication varies widely in different settings. It is far less important when 'strolling through Central Park' than when 'in the confines of one's own home' or when persons are 'powerless to avoid' it."[182] Surely, people "reasonably" think of computers and the personal data stored therein as "at home." And people who contact one on-line site surely have a reasonable expectation that they are still "at home" except for having connected to that particular site. A reasonable consumer user, even if concerned about privacy matters, would hardly expect communication to that site to be greeted by the Web site's application of a "cookie" or even a "Web bug" and gather information to be disseminated to other sites, perhaps for profit.[183]

In the abortion-rights context, the Court categorizes the "unwilling listener's interest in avoiding unwanted communication" as a subset of the broader *right to be let alone*. Labeling Justice Brandeis as one of our wisest justices, the Court says he valued the right to be let alone as "the most comprehensive of rights and the right most valued by civilized men."[184] Information coming to an on-line user from third parties which have been referred by Web sites actually contacted by the user would be incoming information, but still unwanted communication. From the Court's saying that the right has special force in the privacy of the home to avoid unwelcome speech, one needs to imply, regarding data privacy, *unwelcome* rendition.

---

182. *Hill*, 530 U.S. at 716 (citing Cohen v. California, 403 U.S. 15, 21-22 (1971)).

183. On "linking" and "framing" see http://www.cdt.com. *See also* John Schwartz, *Giving Web a Memory Costs Its Users Privacy*, N.Y. TIMES, Sept. 4, 2001, at A1 (explaining "cookies" and "Web bugs").

184. *Hill*, 530 U.S. at 717 (citing Olmstead v. United States, 277 U.S. 438, 478 (1928)).

An urgent difference exists between the *Hill* protesters' speaking freely, on the one hand, and advertisers freely communicating their views, on the other hand. The first implicates individual free speech, and the second, commercial speech. The two perspectives are similar, of course, inasmuch as the speakers are communicating their expression of views. In the context of abortion protest, though, the Court announced that the right to privacy includes the right to avoid unwelcome communication. By extension, then, the right to data-gathering and data-dissemination sought by business interests under First Amendment protection is for data exploitation, not commercial expression. After all, data-distributors more often than not reveal information not their own but belonging to the on-line consumer user. If the right to privacy takes primacy in *Hill*, then *a fortiori* the right to privacy regarding one's on-line personal data must trump another party's alleged right to disseminate that information without the user's prior knowledge and consent.

With *Hill* as legal preliminary, perhaps no case better illustrates the internationality of free-speech legal problems created by cyberspace movement of information than the emotionally charged dispute over worldwide advertising of Nazi memorabilia on U.S.-hosted Yahoo.com. Two French groups advocated censorship by asking a French court to order Yahoo to close access in France to information about the sale of Nazi memorabilia broadcast on Yahoo.com's worldwide sites.[185] The principle before the court was whether the French government had the

185. Jean Eaglesham & Robert Graham, *French Court Ruling Hits Yahoo!*, FIN. TIMES, Nov. 21, 2000, at 1, 21. The International League Against Racism and Anti-Semitism (LICRA) and the Union of French Jewish Students (UEJF) complained that Yahoo! had become the primary retailer for Nazi buffs. *Id. Un juge refuse de financer le process de l'UEJF contre Yahoo! aux Etats-Unis,* AGENCE FRANCE PRESSE, mars 8, 2001 (Paris). "Le Tribunal de grande instance de Paris a refuse jeudi d'accorder une aide financier de 100.000 euros demandee par l'Union des etudiants juifs de France (UEJF) pour aller plaider contre le site Yahoo devant un juge californien." Le portail internet americain Yahoo Inc. a en effet demande a la justice americaine de juger inapplicable aux Etats-Unis car non conforme a loi americaine, la decision rendue le 20 novembre 2000 par le Tribunal de Paris, lui ordonnant de render inaccessible aux internautes francais son site d'encheres permettant d'acheter des objets a caractere nazi. *Id. Sites a contenu nazi fermés sur internet l'organisation "Enfants de l'Holocause" ouvre l'oeil,* SCHWEIZERISCHE DEPESCHENAGENTUR AG (SDA), Service de bas francais, 6 fevrier 2001. "Le fournisseur americain Yahoo!-Geocities a ferms 44 sites internet a contenu nazi depuis l'automne dernier, a annonce mardi l'organisation 'Enfants de l'Holocauste'." *Id.* President Chirac called for a universal international law of the Internet and commented on the recent Yahoo contretemps concerning the sale of Nazi memorabilia on the Internet in France. Laure Noualhat & Edouard Launet, *Chirac pour un "cadre universel,"* LIBERATION, Jan. 12, 2001, at 31.

right to force, extraterritorially, Yahoo to carry out its attempts at information censorship.[186]

III. EU DATA PRIVACY PARADIGM

The EU's current view, embodied in the 1995 Data Privacy Directive 95/46/EC, is the culmination of over fifty years of Western European devotion to recognizing, maintaining, restoring, and ensuring personal privacy. Because the history of this devotion is important to an understanding of the current view, we briefly describe below several key elements.

Almost immediately after the end of World War II, for example, the civilized world was stunned by revelation of barbarous acts attending the war. The victorious allies and the soon-to-be formed United Nations General Assembly quickly went to work to produce the Universal Declaration of Human Rights.[187] Article 12 of the Declaration states, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[188] Article 19 declares, "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."[189] And, according to

186. Because the Internet is global and current laws are not, the French government's attempt to regulate Yahoo's cyberspace activities highlights inevitable questions of jurisdiction over Internet matters. It also raises thorny issues of private-international law (called "conflicts of laws" in the U.S.) which in turn produce clashes of cultural sensitivities. But, in the U.S. at least, notwithstanding obvious conflicts of law, it seems fairly clear that courts would rule that Yahoo would have a First Amendment right to disseminate information, including historically important Nazi symbols and propaganda, as part of the protection the Constitution affords commercial speech. *See, e.g.*, Sean Dodson, *Web Watch: Pardon,* THE GUARDIAN, Dec. 7, 2000. One of the experts in France's Yahoo-Nazi memorabilia case, Ben Laurie, made a clarifying apology about the testimony he submitted to the French court, which apology can be found at http://www.apache-ssl.org/apology.html. Some of the controversy surrounding the French case can be accessed at Sean Dodson, *Web Watch: Nazi Trial,* THE GUARDIAN, Aug. 17, 2000. In addition, in November 1999, America-domiciled Amazon.com acceded to German demands to cease shipping copies of Hitler's *Mein Kampf* to Germany because Germany's laws prohibit all Nazi symbols and imagery. Carl Honori, *Should Nazi Items Be Off-Limits on Net?,* CHICAGO SUN-TIMES, Aug. 10, 2000.

187. Universal Declaration of Human Rights, G.A. Res. 217(a) (III), U.N. GAOR, 3d Sess., U.N. Doc. A/810, at 71 (1948).

188. *Id.*

189. *Id.*

Article 8, "Everyone has the right to an effective remedy by the competent national tribunals for acts violating the fundamental rights granted him by the constitution or by law."[190]

Another direct result of exposure to the carnage of World War II, was the European Convention for the Protection of Human Rights and Fundamental Freedoms ("European Convention on Human Rights").[191] The original six member-state signatories of the European Economic Community[192] (but not the Community itself) were signatories to the Convention on Human Rights. This international convention, signed in the rubble of World War II, establishes the European Court of Human Rights which still sits in Strasbourg, France. Each member state of the first six states constituting the EEC is, and was, also a signatory to the European Convention on Human Rights. In the "Maastricht I" Treaty on European Union (TEU) (now supplanted by the Treaty of Amsterdam) and "Maastricht II" (The Treaty of Amsterdam), the EU itself has still not signed the convention, but this is a technicality. The current Treaty of Amsterdam declares in Article 6 *(ex* Article F*)*, "The Union is founded on the principles of liberty, democracy, respect for human rights and fundamental freedoms, and the rule of law, principles which are common to the Member States." Article 6(2) (*ex* Article F(2)) provides, "The Union shall respect fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms signed in Rome on 4 November 1950 and as they result from the constitutional traditions common to the Member States, as general principles of Community law." Article 49 (*ex* Article 0) makes violations

190. *Id.*

191. European Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 221, revised by Protocol 11 [hereinafter European Convention on Human Rights] (establishing under Article 19 the permanent European Court of Human Rights (sitting in Strasbourg, France)). The Convention is the achievement of the postwar Council of Europe, the first post-war pan-European parliamentary assembly. The Convention was signed in Rome on November 4, 1950 and entered into force in 1953. Almost all the signatory countries to the Convention have incorporated its terms into municipal (national) law.

192. Treaty Establishing the European Economic Community, Mar. 25, 1957, 28 U.N.T.S. 3. (EEC Treaty of Rome) (entered into force Jan. 1, 1958). First called EEC, then EC, the Community signed the Single European Act amending the Treaty of Rome. Single European Act 1987 O.J. (L 169) 1 (1987) (establishing the 1992 Single Market Programme). Since signing the Treaty on European Union, the Community is usually referred to as the EU or European Union. Treaty on European Union, Feb. 7, 1992, O.J. C 224/1 (1992) [hereinafter EU Treaty or Maastricht I]. Then the Community adopted the Treaty of Amsterdam ("Maastricht II"). Treaty of Amsterdam, Oct. 2, 1997, O.J. C 340/1 (1997) *available at* http://www.Europa.eu.int/eur-lex/en/treaties/dat/ec_cons_treaty_en.pdf.

by the EU institutions justiciable, while Article 7 (*ex* Article F(1)) gives power to suspend the Community rights of any Member State which engages in persistent and serious breach of these fundamental principles. The European Convention on Human Rights has this to say about personal privacy:

> Article 8. Right to respect for private and family life. 1. Everyone has the right to respect for private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The European Convention on Human Rights has this to say about Freedom of Expression:

> Article 10. Freedom of expression. 1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises. 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

Pertinent to a discussion of American privacy is this language of the Organization of American States' American Convention on Human Rights:

> Article 11. Right to Privacy. 1. Everyone has the right to have his home respected and his dignity recognized. 2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation. 3. Everyone has the right to the protection of the law against such interference or attacks.
>
> Article 13. Freedom of Thought and Expression. 1. Everyone shall have the right to freedom of thought and expression. This right shall include freedom to seek, receive, and impart information and ideas of

> all kinds, regardless of frontiers, either orally, in writing, in print, in the form of art, or through any other medium of his choice. . . . 3. The right of expression may not be restricted by indirect methods or means, such as the abuse of government or private controls over newsprint, radio broadcasting frequencies, or equipment used in the dissemination of information, or by any other means tending to impede the communication and circulation of ideas and opinions.[193]

Only gradually did the Court of Justice of the embryonic EEC, later the EU, enunciate a system of fundamental freedoms and human rights for the Community, impelled mostly by the Germans who insisted that the German Constitutional guaranties be recognized by the European Court of Justice. Today, in the Treaty on European Union and the subsequent Amsterdam Treaty, the EU might as well have itself become a signatory to the European Convention on Human Rights. And so it might be said without exaggeration that almost from the outset the EU, as with its member states, has insisted on an unambiguous declaration of the individual's right to privacy.[194] Moreover, in the EU, the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (January 28, 1981) began to extend this right of privacy to personal data.[195]

Finally, in 1995 the EU more fully gave its imprimatur to this position through the Data Privacy Directive's Article 1: "Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data."[196] The Directive is based in part on *ex* Articles 100a and 113 of the Treaty.[197]

---

193. American Convention on Human Rights, Nov. 22, 1969, 1144 U.N.T.S. 123.

194. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individual with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) ¶ 10.

195. *Id.* ¶ 11. Parenthetically, in the year 2000, the Council of Europe proposed a convention on the regulation of "cyber crime." European Convention on Cybercrime, Nov. 23, 2001, Europ. T.S. No. 185 (The U.S. is a signatory to this convention, which is expressly opened for signatures by the member states of the Council of Europe and by non-member States which have participated in its elaboration).

196. The 1995 EU Data Privacy Directive is officially called the "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individual with Regard to the Processing of Personal Data and on the Free Movement of Such Data," 1995 O. J. (L 281) 23/11/1995, at 0031-0050, art. 1.

197. *Id.* at Statement of the Council's Reasons § 1 (Introduction).

A. Directive 95/46/EC

With this brief history as background, we now offer the following skeletal five-section overview of the 1995 EU Data Privacy Directive:

1. *Scope.* In its broadest sense the Directive applies to fully or partly automatic processing of personal data and to any manual processing of personal data which forms or is intended to form part of a filing system. There are well-reasoned exceptions, including data processing specifically for household or personal reasons, for journalism or artistic expression, and for reasons of public safety, defense, national security, and criminal activity.[198]

2. *Subject Rights.* Articles 7 and 10-15 of the Directive contain what is arguably the most important discussion in the entire document, enumerating the certain rights individuals may expect. They set out conditions under which personal data may be processed by data controllers, such as businesses and governments, and their data processing agents, such as advertising agencies:[199]

   a. The data subject has given his or her consent unambiguously;

   b. The purpose of the data processing is legitimate;

   c. The data subject knows the identity of the controller and the purpose of the processing;

   d. Data subjects have a guaranteed right to access their data from the controller;

   e. Subjects have the right to object to the processing of their personal information, including such cases as they believe their information will be used in direct marketing; and

   f. Subjects have the right not to be subject to decisions affecting them based solely on automated processing of data intended to evaluate such intangibles as their work performance, creditworthiness, and reliability.

3. *Controller Obligations.* The subsequent Safe Harbor Agreement is concerned with two Directive articles dealing with controller obligations. These obligations are intended to achieve two broad purposes.

---

198. Council Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individual With Regard to the Processing of Personal Data and on the Free Movement of Such Data," 1995 O. J. (L 281) 23/11/1995, at art. 3, and rationalizing the positions, ¶¶ 12-17, 27, and 37.

199. Justifying discussion for these conditions is found in *id.* ¶¶ 25, 26, 28, 30, 31, 33, 38, 39, 41-44, and 69.

First, Article 16 is intended to prevent persons under a controller's authority, for instance employees and subsidiaries, from processing private information without specific instructions from the controller, unless required to do so by law.[200] Second, Article 17 requires controllers to implement technical and organizational measures, consistent with the level of security appropriate to risk, that protect personal data from destruction, accidental loss, unauthorized alteration, disclosure or access over a network, and unlawful processing.[201]

4. *Third Countries.* Thus far the Directive's discussion has centered on Member States, but Article 25 (1) takes up the thorny extraterritorial issue of transfer of personal data to non-Member States.[202] It is this Article, in conjunction with Article 17 from the previous section, that plays such a prominent role in the Safe Harbor Agreement. For it requires that Member States permit transfer of personal data only if the receiving non-Member State ensures an adequate level of privacy protection.[203] This, of course, is a sweeping extraterritorial requirement, stipulating as it does a minimum level of data privacy protection consistent presumably with the EU's own. And that level of data protection is defined in Article 6 and Article 25 (2) in such broad terms that, save for the extraterritorial mandate, it would be difficult to disapprove.

5. *Violations and Remedies.* In the event that controllers or their agents violate rules required by the Directive, two levels of remedy come into play. If, for instance, a violation occurs within a Member State,

---

200. *Id.* ¶ 19.

201. *Id.* ¶¶ 50-54.

202. *Id.* ¶¶ 20, 21, and 56.

203. As an example, consider the hypothetical case of Jaguar, a British firm, and Ford, its American parent. Most companies gather and analyze data they collect from their customers. Their analyses permit them to tailor future advertising and promotion programs to former buyers and to potential new buyers whose personal characteristics conform to previous buyers. Jaguar's use of personal data, of course, is now strictly governed by the British laws implementing the Directive. It is customary, however, for subsidiary firms like Jaguar to transmit customer information to their parent firms for further analysis. If Ford causes Jaguar to transmit its customers' data to New York, Ford as the extraterritorial recipient would in theory be required to stipulate to American authorities that it would act in conformance with the Directive. If Ford, on the other hand, acting in its own best interests and in conformance with U.S. laws only, would not make that stipulation and/or did not in fact act in conformance with the Directive, Britain in theory would be obliged to deny Ford access to information it owns through its Jaguar subsidiary. *See* Marsha Cope Huie & S.D. Hogan, *EU Data Privacy and the U.S. Constitution–the U.S. Perspective*, EU FOCUS, Sept. 7, 2000, at 2.

Articles 22 and 23 require that Member States provide in their own national laws for the right to a judicial remedy and for victims to receive compensation from controllers for any damage suffered. On the second level, Article 25 (3-6) sets out the requirements when a violation occurs in a Non-Member State.[204] If the EU Commission concludes that a violation has occurred, Member States are required to take steps to prevent transfer of the same type of data to the country where the violation occurred. For its part the EU Commission is charged with negotiating with the Non-Member State in order to remedy the situation. As a result of the negotiation, the Commission may conclude that the third country's laws or international commitments are adequate for the protection of basic freedoms and rights of individuals. It remains in that case for the third country merely to enforce its laws and commitments as required in Article 22.

IV. SAFE HARBOR AGREEMENT

A crucial point for this essay is the consequent Safe Harbor Agreement[205] between the U.S. Department of Commerce and the European Commission, the executive arm of the European Union.[206] Below we briefly examine the agreement and the status of U.S. privacy rules almost two years after its entry into force.

---

204. Council Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individual With Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) ¶¶ 57-60.

205. The Safe Harbor Agreement was released as "Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the U.S. Department of Commerce (notified under document number C (2000) 2441)," Commission Decision 2000/520/EC, 2000 O.J. (L 215), 25/08/2000 at 0007-0047. The EU Web address of the Working Party is: http://www.europa.eu.int/comm/internal_market/en/mediaprot/wpdocs/index.htm.

206. The Council is the legislator of the EU in that the Commission, with its right to initiate legislation, must submit proposed legislation to the Council, which must then consult, cooperate, or co-decide with the European Parliament, depending upon the nature of the proposed legislation. The EU Commission is charged with ensuring that the constitutive treaties of the EU are followed and keeping the EU institutions moving in accord with the treaty dictates. EU Treaty Articles 81-88 (*ex* 85-93) make the Commission the executive regarding Community competition policy. Playing the major role of the community, the Commission has the power to issue its own decisions. The supervisory Commission's members are to represent the *community* interest, not the national interests of the various member states which are necessarily represented by the EU Council members. Its mission is to be every bit as integrationist for the Common Market as is the European Court of Justice. EU Treaty, *supra* note 192, at art. 226 (*ex* Art. 169).

The Safe Harbor Agreement (the Agreement) represents acceptance by the EU Commission in July 2000, of the U.S. Department of Commerce's proposed Safe Harbor Privacy Principles[207] relating to U.S. protection of data privacy. It is the culmination of years of negotiation over application of the Privacy Directive to the U.S., and reflects the U.S. government's assurance that privacy had, in the view of the Commission, met EU requirements of adequate protection for privacy. The Commission, however, left open the right to re-think the Agreement's framework in the event the EU Parliament's fears of inadequate individual remedies were realized. Earlier, on July 5, 2000, the EU Parliament had issued a non-binding opinion which objected to EU adoption of the U.S. safe harbor principles because Parliament believed the U.S. system failed to provide adequate prophylaxis and remedies for an individual whose privacy had been violated.[208]

The Agreement presents the following seven privacy principles, along with several indispensable "Frequently Asked Questions" ("FAQs") and the FTC's responses:

1. *Notice.* In order to order to qualify, a U.S. organization must tell individuals in clear and conspicuous language why it is collecting and using personal data about them, and how to contact the organization with inquiries or complaints. It must also notify the affected individuals the names of the parties to which it sells or otherwise transfers those personal data, along with the choices and means available to the individual for limiting use and disclosure of the data.

FAQ2 and response relate to notice required when personal data would be used for journalistic purposes. The FTC holds that whenever "the rights of a free press embodied in the First Amendment to the U.S. Constitution intersect with privacy protection interests, the First Amendment must govern the balancing of these interests" regarding the activities of U.S. citizens and organizations. Information gathered for

207. Released as "Safe Harbor Privacy Principles issued by the U.S. Department of Commerce on July 21, 2000." Commission Decision of 26 July 2000, *supra* note 205.

208. The EU Parliament (EP) voted 279 to 259 in favor of a report of one of its consumer-rights committees critical of allowing transmittal to the U.S. of EU personal data, because the EP perceived inadequate the U.S. privacy safeguards in place for personal information. The EU Commission, however, was not bound by the EP's negative vote, because the EP's powers were limited to whether the EU Commission had followed proper procedures in negotiating and drafting the Safe Harbor Agreement. Robert MacMillam, *EU, European Parliament Tussle Over Data Privacy*, NEWSBYTES, July 7, 2000, *available at* http://www.newsbytes.com.

publication, broadcast, or other forms of public communication of journalistic material is, therefore, not subject to the Agreement.

2. *Choice.* A qualifying U.S. organization must also offer the individual, clearly and conspicuously, an effective opportunity to opt out of (1) the disclosure of the personal data to a third party and (2) any use of the data which is incompatible with the use for which the data were originally collected or for which the individual authorized use. For sensitive personal data,[209] the opt-out option is not sufficient. Rather, the individual must have an explicitly affirmative opt-in option if the information is to be disclosed to another party or used for some purpose other than its originally declared purpose.

The FTC's response to FAQ1 holds that the opt-in choice is not always mandatory with sensitive data. The exceptions include when processing is (1) in the vital interests of the individual involved, (2) necessary to establish legal claims or defenses, (3) required for medical care, (4) necessary to carry out the organization's obligations relating to employment law, and (5) related to data already made public by the individual.

3. *Onward Transfer.* If organizations wish to disclose private information to a third party, such as a subsidiary or business partner, organizations must apply the Notice and Choice principles above. Moreover, they must determine that the third party subscribes to the Agreement in practice or in principle. Organizations thus transferring personal data cannot be held responsible if the third party henceforward violates the spirit or the understanding, unless the organization knew or should have known that the third party would do so.

4. *Security.* According to the Agreement, "[O]rganizations creating, maintaining, using, or disseminating personal information must take reasonable precautions to protect it from loss, misuse, and unauthorized access, disclosure, alteration, and destruction."

5. *Data Integrity.* Personal information should be relevant for the purpose it was gathered, and should not be processed if the purpose is incompatible with the purposes for which it was gathered and authorized. In addition, organizations should take the necessary steps

209. The Safe Harbor Agreement defines "sensitive information" to include medical or health conditions, racial or ethnic origins, political opinions, religious or philosophical beliefs, trade union membership, or information about individuals' sex lives.

to ensure that any collected data are accurate, complete, and current.

6. *Access.* Individuals must have access to the personal information about themselves so they may correct, amend, or delete any information about them that is not accurate. A qualifier to that principle is that the cost of providing access must be proportionate to the individual's privacy, or where other individuals' right to privacy would be compromised.

7. *Enforcement.* In general, the Agreement insists that, to be effective, privacy protection must include mechanisms for assuring compliance with the Principles, recourse for individuals who have been adversely affected by violation, and consequences for organizations in violation. These mechanisms must be readily affordable and independent of the violating organization. And sanctions, in the language of the Agreement, "must be sufficiently rigorous to ensure compliance by organizations."

A U.S. organization may qualify for the Safe Harbor Agreement in one of two, strictly voluntary ways. It may, for instance, adhere to the privacy principles by publicly declaring an intent to do so and by joining a self-regulatory privacy program, such as a trade group's code of privacy, or by developing its own self-regulatory policy, thus certifying itself. Or it may qualify if it is subject to a legally binding law or rule which protects personal privacy. In the case of self-certification, an organization's breach of the Agreement is actionable under the FTC Act or any other applicable U.S. law.[210] The U.S. business must think hard before placing itself on the Safe Harbor list and subjecting itself to the jurisdiction of the FTC for breach of its own stated privacy policy.

In all cases the U.S. organization seeking to qualify for the safe harbor benefits receives them on the date of self-certification to the Department of Commerce. Then, according to the Privacy Principles, "U.S. law will apply to questions of interpretation and compliance with the Safe Harbor Principles (including FAQs) and relevant privacy policies by safe harbor organizations. An exception exists where organizations have committed

210. Federal Trade Commission Act, § 5, declares illegal "unfair or deceptive acts or practices in or affecting commerce" and confers on the FTC the plenary power to prevent such acts and practices. *Id.* Thus, the FTC has the authority "to take action against those who fail to protect the privacy of personal information in accordance with their representations and/or commitments to do so." FTC Safe Harbor Privacy Principles, *supra* note 207.

themselves to cooperating with European Data Protection Authorities."[211] In the latter case EU law will apply.[212]

A. Directive Article 26 and Standard Contractual Clause Provisions

The EU Commission has recently adopted model contractual clauses, by a Commission Decision controversial in the U.S. If used by business on a contract-by-contract basis, these contractual clauses guaranteeing data privacy will satisfy Article 26 of the 1995 EU Data Privacy Directive.[213] The Commission's decision decrees that use by a U.S. business of these proposed standard contract clauses, as an alternative to a company's bringing the business' privacy policy within the Safe Harbor provision established in Article 25 of Directive 95/46/EC, will pass muster under Article 26 of Directive 95/46EC. According to Representative Billy Tauzin, Chair of the U.S. House of Representatives Committee on Energy and Commerce, speaking on March 8, 2001, "The EU's data-privacy efforts for e-commerce could. . .[impose]. . .one of the largest free trade barriers ever seen." Despite protestations by the George W. Bush Administration about these proposed model contractual clauses, the EU Commission nevertheless chose to adopt them. If the George W. Bush Administration continues, post-September 11, to view the Safe Harbor and Directive Article 26 arrangements as "trade barriers" and the EU were to levy "trade sanctions" and the U.S. were then to retaliate by assessing its own trade sanctions, would a "trade war" ensue? That is the fear often expressed.

It seems apposite here to mention an extraterritorial provision of the new "Patriot" or Anti-Terrorism Bill which President Bush signed into U.S. law on October 26, 2001.

> Section 319. Forfeiture of Funds in United States Interbank Accounts.
>
> (a) Forfeiture from United States Interbank Account . . .
>
> (k) Interbank Accounts

---

211. Council Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individual With Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281).

212. The constitutive treaties of the EU compose what might be loosely called the "constitution of the EU."

213. Letter from the U.S. Dept. of Commerce and U.S. Treasury Dept. to the EU Commission, *supra* note 21 and accompanying text; *see also* Paul Kilmer, *European Union Adopts Standard Contract Clauses for Transfer of Personal Data* (Oct. 25, 2001), *available at* Mondaq, Ltd., http://www.mondaq.com. The U.S. Department of Commerce provides instructive information about these model contractual clauses on the Web at http://www.export.gov/ safeharbor/sh_modelcontract.html.

(1) In General

(A) In General—For the purpose of a forfeiture under this section or under the Controlled Substances Act (21 U.S.C. § 801 et seq.), if funds are deposited into an account at a foreign bank, and that foreign bank has an interbank account in the United States with a covered financial institution . . . the funds shall be deemed to have been deposited into the interbank account in the United States, and any restraining order, seizure warrant, or arrest warrant in rem regarding the funds may be served on the covered financial institution, and funds in the interbank account, up to the value of the funds deposited into the account at the foreign bank, may be restrained, seized, or arrested. . . .

(2) No Requirement for Government to Trace Funds–If a forfeiture action is brought against funds that are restrained, seized, or arrested under paragraph (1), it shall not be necessary for the Government to establish that the funds are directly traceable to the funds that were deposited into the foreign bank, nor shall it be necessary for the Government to rely on the application of section 984.[214]

The extraterritorial reach of the U.S. statute is obvious.

V. CONCLUSION: ACHIEVING BALANCE OF INTERESTS BY EITHER ENACTMENT OF AN OVERARCHING NATIONAL DATA-PRIVACY STATUTE OR FRANK ADOPTION OF A PRIVACY AMENDMENT TO THE U.S. CONSTITUTION

Three avenues exist for U.S. business to receive data flows from the EU under Directive 95/46/EC and the Safe Harbor Agreement executed between the EU and the U.S. First, the entire U.S. nation could enact comprehensive privacy laws so as to achieve certification by the EU, as have our NAFTA partner Canada, and Hungary and Switzerland. Their national privacy laws have allowed them, and indirectly their companies, to be certified by the EU as third-party states to which onward transfer from the EU of personal data can be freely made.

Regarding this first avenue for U.S. business to comply with the EU Data Privacy Directive, we have shown here that in the U.S. the "commercial free speech" argument made under the First Amendment to the U.S.

214. Antiterrorism Bill, § 319, H.R. 3162, 107th Cong. (2001) (signed into law by President George W. Bush, Oct. 26, 2001).

Constitution might render ineffective an effort either to join as signatories an international treaty on data privacy, or to enact a comprehensive national privacy law designed to protect personal information in general, and stored in electronic documents in particular, from intrusive business eyes. If such an overarching U.S. national privacy statute were to be declared unconstitutional, then consumer data in the U.S. could continue to be gathered, used, and disseminated by organizations without the knowledge or permission of the U.S. data subject.

We fear that the same fate, a judicial finding of unconstitutionality, might befall an international convention, signed by the U.S., designed to protect the privacy of personal data. On the nature of such an international treaty, we refer the reader to Fordham University law professor Joel Reidenberg. He argues that international data-privacy standards might be adopted through the World Trade Organization.[215]

For now, as a second way for U.S. business to receive data flows from the EU even under the EU Data Privacy Directive, a particular U.S. business can voluntarily list itself on the Safe Harbor list maintained by the U.S. Department of Commerce. This act of "self-certifying" places the business and its adherence to its stated privacy policy under the scrutiny of the FTC. This method, an alternative for other means of compliance with EU Directive 95/46/EC, is a short-term, stopgap measure. As such, it should be easier and less expensive for U.S. business than doing what is ultimately in the interest of U.S. mercantilism: persuading Congress to enact national privacy legislation assuring the EU that adequate privacy safeguards are in place in the U.S. to satisfy the EU directive. Article 26 of Directive 95/46/EC says that adequacy of data-privacy protection is to be determined from surveying the third country's laws. But U.S. laws, contended the EU Parliament, did not include the Safe Harbor Agreement at the time the EU Commission enacted the 1995 Data Privacy Directive. Nevertheless, as mentioned, the EU Commission chose to sign the Safe Harbor Agreement with the U.S. Government.[216]

---

215. *See* Joel Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, 38 HOUS. L. REV. 717 (2001).

216. EUR. PARL. DOC. R5 305, 2-3 (2000); the official EU cite for the Safe Harbor Agreement as published by the EU in July 2000 is the Commission Decision of 26 July 2000, *supra* note 205 (comprising Safe Harbor Privacy Principles and FAQs, as well as several addenda and representations made to the EU Commission by the U.S. FTC and U.S. Department of Commerce). In the U.S., *see* Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45,665, 45,665-45,686 (July 24, 2000). The Safe Harbor Agreement is inapplicable to EU telecommunications and financial-services institutions, and U.S. FTC jurisdiction excludes these sectors, too.

As a third alternative for satisfying the 1995 EU Data Privacy Directive, a U.S. business can avail itself of Article 26 of Directive 95/46/ EC and submit its contracts for approval by the EU Commission. This third avenue has been facilitated by the EU Commission's controversial adoption in 2001 of its proposed non-mandatory Standard Contractual Clauses. Use of these standard contractual clauses by U.S. businesses will allow EU data controllers to transmit data to the complying U.S. business.[217]

The 1995 EU Data Privacy Directive (EU Directive 95/46/EC), with its extraterritorial application worldwide, will probably lead to a *de facto* informational privacy standard for the world, creating a new international law for data privacy.[218] How will this new *ius gentium* become adapted to the United States legal system?

Is it possible to achieve balance between the rights of commercial speech and data privacy? Having argued throughout this article that the importance to society of the latter outweighs the former, we are sanguine about achieving harmony of the two interests, even as calls for governmental intrusions mount as a result of the September 11 terrorist attacks.

Two U.S. approaches, tried in sequence, may succeed in achieving that desired balance. First, Congress might enact a comprehensive national data-privacy statute, although efforts to do so have been stalled too long in the U.S. Congress. Upon enactment of a data-privacy statute, the question then becomes whether the Supreme Court would find such a statute unconstitutional (as impermissibly restricting business' so-called right of commercial free speech) under any of the Court's traditional tests for constitutionality of a governmental regulation.

The Supreme Court's three tests in ascending order of scrutiny are the so-called rational-basis test, the middle-tier analysis, and the strict-scrutiny analysis. If the Court were hesitant to apply any of its three traditional tests in a way so as to find a data-privacy statute constitutional, the Court could frankly apply a European-style principle of proportionality to save the statute. It should even be possible, though, for the U.S. Supreme Court to recognize the primacy of the principle of data privacy over commercial free speech through a means-to-end test less close to the strict-scrutiny test than to what is often described as the middle-tier test for examining the

---

217. *See* Kilmer, *supra* note 213 and accompanying text.

218. Peronet Despeignes & Deborah Hargreaves, *The Americas: U.S. Criticises EU on Data Privacy,* FIN. TIMES, Mar. 9, 2001, at 12 (quoting U.S. Congressional Representative Billy Tauzin). EU Data Privacy restriction has not yet been imposed on any U.S. company or Web site of consequence but, according to Rep. Tauzin, could lead to effective imposition of a "de-facto privacy standard on the world." *Id.*

constitutionality of a government action.[219] The European test used by the European Court of Justice in the Skimmed Milk Powder[220] case, discussed a bit below, would suffice. The personal right to informational privacy is so important to 21st-century society that if Congress' attempt to enact a "constitutional" statute fails for any reason, the U.S. should enact a constitutional amendment guaranteeing the right, with only "strictly necessary" safeguard or escape hatches.

A. The European Principle of Proportionality

Regarding the constitutionality of a properly written, narrowly tailored U.S. data-privacy statute, a proper balance could be struck if modest compromises obtain through application of what the Europeans call a "General Principle of Proportionality." This judicial construction would allow only limited ("strictly necessary") business on-line or offline intrusions into personal privacy, a fundamental human right. This same principle of proportionality has been recognized by the German constitutional court in interpreting the post-war German constitution, as well as by the broader EU jurisdictions.

The European principle of proportionality balances the ends to be achieved by *loi* or law against the burden imposed by the government's regulation. The burden imposed must be no greater than is *"strictly necessary" in the public interest* to achieve the end desired by the law. As mentioned, in the EU regime, for example, a business may not hold personal data longer than is "strictly necessary."

---

219. In the U.S., the easiest judicial analysis under the Fifth and Fourteenth Amendments of the U.S. Constitution for upholding a statute or regulation seeks only a *rational basis* between the attempted regulation and a governmental interest advanced by the regulation, while the strictest-scrutiny test of a statute asks whether the regulation affecting a "suspect classification" satisfies a *compelling* state interest in enacting the regulation. *Compare* the "rational basis" test, "strict scrutiny" test, and "middle-tier" test applied by the U.S. Supreme Court. "Rational basis" test–lowest level; the statute must only bear some rational relationship to the legitimate government interest in order to be upheld. *See* New Orleans v. Dukes, 427 U.S. 297 (1976) and City of Cleburne v. Cleburne Living Center, 473 U.S. 432 (1985). "Middle-tier" test: An intermediate standard requiring that the government's "important state interest" objectives must be substantially related to the means of achieving the objectives. *See* Mississippi University for Women v. Hogan, 458 U.S. 718 (1982) and Craig v. Boren, 429 U.S. 190 (1976). "Strict Scrutiny" test: The government must have some compelling interest as its objective and there must be no other less discriminatory means by which to achieve the objective when the law impinges upon a fundamental right such as the right to privacy or a "suspect classification" such as race or national origin. *See* Loving v. Virginia, 388 U.S. 1 (1967) and Regents of University of California v. Bakke, 438 U.S. 265 (1978).

220. Bela-Mühle Josef Bergmann KG v. Grows-Farm GmbH & Co., 1977 E.C.R. 1211, 2 C.M.L.R. 83 (1977) (Skimmed Milk Powder Case).

Under U.S. judicial middle-tier analysis, the government seeking to regulate an activity such as on-line data gathering must show that its means (method) is substantially related to achieving an important governmental interest. If the EU general principle of proportionality were to be imposed in the U.S., as some case law seems to indicate,[221] the principle promises a least-intrusive (i.e., highly reasonable) means test for government action. This sounds a bit closer to the U.S. strict-scrutiny test than to the U.S. mid-level scrutiny test to protect the fundamental human right to privacy.

Surely the U.S. can glean much wisdom from the horrors of the Nazi experience concerning the right to privacy, as has the post-war German Constitutional Court.[222] The post-World War II German Constitutional Court feared that the Community court might fail to respect the fundamental human right of privacy. Openly determined not to sign on unreservedly to the European Court of Justice's assertions of primacy of Community law over conflicting national law,[223] the German Constitutional Court made it clear that the principle of proportionality must be adopted by the Court of Justice to earn full West German compliance with the European Economic Community Court's early EEC rulings.[224] In essence,

---

221. *See* Madsen v. Women's Health Ctr., 512 U.S. 753 (1994); United States v. Bajakajian, 524 U.S. 321 (1998).

222. Germany provided the initiative calling for EU legislation protecting data privacy, to supplement any national privacy legislation already in effect in the EU member states. In 1994, *Newsbytes* reported: "Despite the fact that Germany has, arguably, the most powerful data privacy legislation in Europe, the government has revealed it is worried about the pace at which computer and communications technology are eroding personal privacy." Sylvia Dennis, *German Government Worried About Data Privacy Legislation*, NEWSBYTES, Dec. 2, 1994.

223. Costa v. ENEL, 1964 E.C.R. 585, 1964 C.M.L.R. 425 (establishing principle of supremacy of Community law over conflicting member-state law). "The transfer, by member-States, from their national order, in favor of the Community order of the rights and obligations arising from the Treaty, carries with it a clear limitation of their sovereign right upon which a subsequent unilateral law, incompatible with the aims of the Community, cannot prevail." *Id.*

224. Stauder v. City of Ulm, 1969 E.C.R. 419 at point 7. The next rather early EU case establishing the requirement of proportionality as a general principle of Community law was Internationale Handelsgesellschaft ("Solange I"), 1970 E.C.R. 1125. In criminal law, the U.S. Supreme Court recognizes the doctrine of proportionality as a general principle of law (Terry v. Ohio 392 U.S. 1 (1968)), but has not specifically done so in civil cases. The Court came close to enunciating a general, European-style doctrine of proportionality in the abortion-picketing case (Madsen v. Women's Health Ctr., 512 U.S. 753 (1994)), when it upheld an injunction issued against abortion-protesters' activities, which restricted the freedom of speech of the protesters by establishing a 36-foot buffer zone (sort of a floating zone of privacy for the woman seeking entrance to the abortion clinic). Then, in the *Bajakajian* forfeiture case, the Supreme Court seemed to apply its own rule of proportionality. United States v. Bajakajian, 542 U.S. 321 (1998).

the national court promised compliance with the Community court only "so long as" (*solangewie*) the latter complied with the German constitutional court's human-rights fundaments.

The *realpolitik* dance of the Court of Justice and the German Constitutional Court delights the legal observer. In *Stauder v. City of Ulm*,[225] for instance, the Court of Justice recognized for the first time that Community law embraces certain fundamental human rights as a general principle of Community law. Second, in *International Handelsgesellschaft*,[226] the Community court proclaimed that national law (German constitutional law) could not dictate Community law. Nevertheless, the Community court offered the "inspired by" olive branch, stating, "respect for fundamental rights forms an integral part of the general principles of law protected by the Court of Justice. The protection of such rights, whilst inspired by the constitutional traditions common to the Member States, must be ensured [by the Community court] within the framework of the structure and objectives [of the Community's laws]."[227]

The Advocate General to the European Court of Justice in *International Handelsgesellschaft* defined the Principle of Proportionality as requiring that the burden (the means) imposed by governmental regulation must be measured against the result to be achieved (the end), and that burden must be strictly necessary in the public interest to achieve the result intended by the regulation. The test of proportionality resembles what the English and Americans might call a proportionality rule of reason: If the means are reasonably related to, and not disproportionate to, the end to be achieved, and reasonably likely to achieve the purpose of the regulation, and if the burden imposed is in the public interest, and no greater than necessary to achieve the end desired, the regulation will be likely to withstand judicial scrutiny.[228] Furthermore, the relationship between the members of the public who are not harmed but

225. *Stauder*, 1969 E.C.R. 419 at point 7.

226. Internationale Handelsgesellschaft GmbH v. Einfuhn-und Vorratsstelle für Getreide und Futtermittel ["Solange I"], 1970 E.C.R. 1125 (EC regulation conflicting with German constitutional provision establishing principle of proportionality). (So long as [*solangewie*] the ECJ employs a satisfactory general principle of proportionality in its analysis, the German Constitutional Court will abide by the otherwise competent decisions of the former. So long as the Court of Justice recognises fundamental human rights, really, then the German Constitutional Court will acknowledge the primacy of EU law in certain, limited areas).

227. *Id.* at 1134 (and so the embryonic federalist union was saved from German retrenchment).

228. *Id.* at 1146 (Opinion of Advocate General Dutheillet de Lamothe). *See* T.C. HARTLEY, THE FOUNDATION OF EUROPEAN COMMUNITY LAW 137 (offering the best early available discussion in English of the EU principle of Proportionality).

aided by the regulation must not be disproportionate in relation to the persons who are harmed by the regulation.[229]

In criminal law, the U.S. Supreme Court expressly recognizes a doctrine of proportionality as a general principle of law, for example in *Terry v. Ohio*.[230] Another interesting case involving a U.S. doctrine of proportionality in a recent criminal forfeiture case is *Bajakajian*,[231] in which the Court applies a kind of proportionality test to a criminal forfeiture case. The Court has not expressly recognized a rule of proportionality in civil cases except civil-forfeiture cases. As a close approximation, in scrutinizing a particular governmental regulation the Court has come close to enunciating a European-like doctrine of proportionality in *Madsen v.*

---

229. An interesting EU case in point is known in English as the Skimmed-Milk Powder case, and officially as Bela-Mühle Josef Bergman v. Grows-Farm, 1977 E.C.R. 1211. At the expense of Community non-milk producers (such as soy milk producers), the EEC, as it then was, imposed a requirement that commercial producers of animal feed had to include a certain amount of skimmed-milk powder in the animal food, making the animal food relatively very expensive. The regulation's purpose: Acting under the Common Agricultural Policy (the CAP), the Community imposed this burden on the non-milk producers in order to reduce the Community surplus of milk products, with the obvious effect of presenting a pecuniary benefit to milk producers. The measure was held by the European Court of Justice to violate the principle of proportionality; the burden imposed was not necessary to reduce the skimmed-milk surplus, and the soya producers were disproportionately disadvantaged. *Id.*

230. Terry v. Ohio, 392 U.S. 1, 17-18 (1968) (establishing proportionality principle as normative approach for Fourth Amendment Search and Seizure Analysis, to demand from government a specific showing of need proportionate to the invasion of the constitutional protection). *See* Christopher Slobogin, *Let's Not Bury Terry: A Call for Rejuvenation of the Proportionality Principle*, 72 ST. JOHN'S L. REV. 1053, 1088 (1998); Judge Richard Posner, *Rethinking the Fourth Amendment,* 1981 SUP. CT. REV. 49 (applying economic analysis best to decide how to achieve Framers' Fourth Amendment goal of deterring overzealous government agents); Enmund v. Florida, 458 U.S. 782, 822 "Eighth Amendment concept of proportionality involves more than merely a measurement of contemporary standards of decency. It requires in addition that the penalty imposed in a capital case be proportional to the harm caused and the defendant's blameworthiness."

231. United States v. Bajakajian, 524 U.S. 321 (1998) (applying a kind of proportionality test to criminal forfeiture case in which "forfeiture" of currency was ordered for violation of a statute requiring a person to report transportation of more than $10,000 currency outside the U.S., is punishment and consequently constitutes a "fine" within the meaning of the Excessive Fines Clause of the U.S. Constitution, Amendment 8; 18 U.S.C.A § 982(a)(1); 31 U.S.C.A. § 5316(a)(1)(A)). The district court concluded that full forfeiture would be grossly disproportional to the offense in question and would therefore violate the Eighth Amendment; affirmed by the Ninth Circuit. Affirmed: Supreme Court held the forfeiture of the entire funds would be grossly disproportionate to the gravity of defendant's offense, which was solely a reporting offense. He violated no U.S. law by transporting the currency from the U.S. so long as he reported it..

Women's Health Ctr.[232] The Court held that an injunction issued against abortion-protesters' activities, which restricted protesters' freedom of speech by establishing a 36-foot buffer zone of privacy, passed constitutional muster as a reasonable restriction on the First Amendment right to picket an abortion clinic. For the Court squarely to say that an overarching national data-privacy statute would be constitutional as a permissible incursion on the First Amendment Free Speech Clause as applied to commercial speech[233] would not require a great leap from the Court's opinion in *Hill*.[234]

Indeed, an omnibus national data-privacy statute is of such fundamental importance that it ought to pass even the U.S. "strict judicial scrutiny" test which demands a compelling need for governmental regulation. Surely this is so, given the reasonable expectation of privacy which the on-line individual should have regarding personal data to foster Internet commerce. Without faith in the privacy of personal data entered on-line, many if not most consumers will refuse to purchase on-line. And arguably, given the gravity of potential invasions of personal privacy rendered possible by Internet operators, the Supreme Court, were it to apply merely its "rational basis" test for vetting the constitutionality of proposed legislation, could surely find with facility that a comprehensive data-privacy statute had a rational basis to advancing a legitimate government interest, as against the barely-born doctrine of freedom of commercial speech.[235]

---

232. Madsen v. Women's Health Ctr., 512 U.S. 753 (1994) (36-foot buffer zone between abortion protesters and abortion-clinic entrances, and injunction limiting protesting noises, held not violative of protesters' First Amendment right to free speech and picketing; but the burden, the means, imposed by a 300-foot buffer zone held constitutionally impermissible as being disproportionately large, unnecessarily restrictive, for serving the interest of the government in regulating First Amendment behavior). The woman's constitutional Right to Privacy prevailed. Schenck v. Pro-Choice Network 519 U.S. 357 (1997) (upholding Madsen's finding that woman's constitutional right to seek abortion justified "appropriately tailored" preliminary injunction so woman could enter abortion clinic, and upholding "fixed buffer zones of 15 feet from clinic access, but rejecting "floating 15-foot buffer zones" as overbroad in that they burdened more First Amendment freedom of protest than was necessary to serve the pertinent governmental interests). *Id.* at 380; Hill v. Colorado, 530 U.S. 703 (2000).

233. The sale-for-profit of a data subject's private information without the subject's knowledge or consent should not constitute "commercial speech" under U.S. case law.

234. *Hill*, 530 U.S. 703 (holding constitutional a state statute impinging on abortion protesters' First Amendment Freedom of Speech, the right to dissuade women from seeking abortions, but designed to protect a woman's constitutional right of privacy allowing her to seek abortion).

235. We take particular note of Professor Krotoszynski's proposal that each state should legislate that no property interest exists in data comprising personal information so that the

The U.S. Supreme Court might choose to achieve the result of holding an omnibus data-privacy statute constitutional by enunciating and adopting a general principle of proportionality allowing only very limited intrusions into personal privacy,[236] essentially the same principle of proportionality as recognized in EU case law,[237] which has allowed the

---

government which regulates data privacy will not be violating the Takings Clause of the U.S. Constitution. And, we commend to the reader his excellent discussion of the failings of technology and the desirability of regulation the intrusions of technology in the interest of human privacy. Krotoszynski, *supra* note 35.

236. Several states' constitutions and statutes provide for protecting the privacy interest. Concerning wording in the Safe Harbor Agreement: *Damages for Breaches of Privacy, Legal Authorizations, and Mergers and Takeovers in U.S. Law* (FTC chairman responding to EU Commission's request for clarification of U.S. law concerning damages for breaches of privacy in U.S. and EU Commission's inquiry concerning "explicit authorizations" in U.S. law which require intrusions of privacy) is available at www.export.gov/safeharbor/privacydamagesfinal: assuring the EU that "the right to recover damages for invasion of personal privacy is well established under U.S. common law"; and "Federal and state privacy legislation often provides private causes of action for money damages" and at note 5, "An electronic search of the Westlaw database found 2,703 reported cases of civil actions in state courts that pertained to 'privacy' since 1995. We [the FTC] have previously provided the results of this search to the Commission. . . . Moreover, at least twelve states have constitutional provisions safeguarding their citizens' right to be free from intrusive actions [his note 6], which in some cases could extend to protect against intrusion by non-governmental entities . . . Some state constitutions include privacy protections which surpass privacy protections in the U.S. Constitution. Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington have broader privacy protection." To state the obvious, though, any federal statute concerning consumer privacy would be overridden by a more restrictive federal statute which intends preemption. Under the U.S. federal system, little consolation exists in the state constitutions. To avoid Supremacy Clause preemption of state legislation, the guaranty of individual data privacy should best be explicitly stated in the U.S. Constitution.

237. Stauder v. City of Ulm, 1969 E.C.R. 419 (on proportionality). In criminal law, the U.S. Supreme Court recognizes the doctrine of proportionality as a general principle of law, (*Terry v. Ohio*), but has not specifically done so in civil cases. The Court came close to enunciating a doctrine of proportionality in the abortion-picketing case of *Madsen*. *See also* United States v. Bajakajian, 542 U.S. 321 (1998) (holding in a forfeiture case). *Analysis: Terrorism Fears Risk Sapping EU Privacy Rules*, REUTERS WIRE, Sept. 26, 2001 (expressing concerns of civil-liberties groups in Brussels, home of the EU Commission, that the war against global terrorism will evoke serious intrusions of privacy by law-enforcement officials). Press Release, Center for Constitutional Rights, Center for Constitutional Rights Warns of Dangers of Providing the President With Vast War Powers: No Time for Cowboy Politics (Sept. 17, 2001), *at* http://www.humanrightsnow.org; Press Release, National Lawyers Guild, *National Lawyers Guild Urges Government to Protect Civil Liberties, Punish Bias Crimes and Refrain from Bombing Civilian Populations During National Crisis* (Sept. 11 2001), *at* http://www.nlg.org ("We must be particularly vigilant during times of national crisis to protect civil liberties. . . .").

1995 EU Data Privacy Protection Directive to stand as "constitutional" under the constitutive treaties of the European Union.

The risk of relying on an overarching national data-privacy statute to withstand constitutional attack is evident. It cannot be gainsaid that any proper balance between data privacy and commercial free speech is necessarily struck within the prevailing socio-political context. As that context changes, so too does the structure in place at the time the first balance was achieved. A case in point is the current Bush Administration's announcement that it may wish to revisit the Safe Harbor Agreement,[238] having concluded that the balance mandated for data privacy was excessively skewed toward individual privacy *versus* commercial free speech. For instance, the letter from the U.S. Department of Commerce quoted in our *introductio* illustrates hostility toward the Safe Harbor Agreement and perhaps evinces an intent completely to revisit the issues so long negotiated before reaching the Safe Harbor understanding in late July 2000.

If the U.S. back-peddles from the Safe Harbor Agreement, it will achieve a symmetry which would then be ironic. For in 1995 the EU almost single-handedly bullied the U.S. into adopting any sort of data-privacy initiative at all, culminating in the EU-U.S. Safe Harbor Agreement executed in late July 2000. Indeed, the EU seemed willing to provoke a trade war over the privacy issue, threatening soon to outlaw its businesses' sending data to the U.S. unless the U.S. made a serious showing of efforts to protect the privacy of personal data. The EU's 1995 directive on data privacy firmly forbade future transmission of data to the U.S. (or any other foreign country) which operated without a regime for effective protection of personal data. Although the U.S. government–then the Clinton Administration–would not admit to it, the U.S. fell in line with the EU and began to move toward adopting serious data-privacy regulation, with the July 2000 Safe Harbor Agreement as a milestone.[239] Now, more than a year after entry into force of the Safe Harbor Agreement, the EU is seeking to extend its protection by enacting legislation requiring collectors of data to

---

238. *Analysis: Terrorism Fears Risk Sapping EU Privacy Rules*, *supra* note 237 (expressing concerns of civil-liberties groups in Brussels, home of the EU Commission, that the war against global terrorism will evoke serious intrusions of privacy by law-enforcement officials). Center for Constitutional Rights, *supra* note 237. National Lawyers Guild, *supra* note 237.

239. The U.S. unblushingly enacted the extraterritorial Helms-Burton Act to impose sanctions on any company located anywhere dealing with Castro's Cuba. *See also* Anti-Terrorism Bill, § 319, H.R. 3162, 107th Cong. (2001). For a concise compilation of extraterritorial case law, *see* Marsha Cope Huie, *Neale & Stephens, International Business and National Jurisdiction*, 12 FORDHAM INT'L L. J. 589 (1989) (book review).

destroy, within months of collection, all data directly or indirectly identifiable to a particular person.[240]

In addition to its belief that the Safe Harbor Agreement too strongly favors individual privacy *versus* commercial free speech, a balance which is of course politically determined, the U.S. government may argue that the exigencies of post-September 11 national safety necessitate abandoning attempts to enhance privacy protections for cyberspace. Certainly U.S. First Amendment interests will bow for a significant time to the government's need to seek and destroy international terrorism. Consider, for example, U.S. Attorney General Ashcroft's proposed curtailments on traditional civil liberties proposed in the wake of the September 11 attacks.[241] The Congress specifically approved the Anti-Terrorism or so-called Patriot Bill with speed which only time will prove to have been too hasty or not. If the U.S. does succeed in weakening the EU-U.S. Safe Harbor Agreement or, citing reasons of national security, is able to persuade the EU to suspend operation of its 1995 Data Privacy Directive, symmetry would be achieved.[242]

B. U.S. Mushrooms Jurisprudence

It is not safe to assume that the United States Supreme Court would find an omnibus national personal-data privacy statute constitutional vis-à-vis other rights asserted by commercial interests. Currently, Supreme Court Free Speech jurisprudence holds that the First Amendment right to advertise cigarettes and mushrooms is stronger, at least on a surface

---

240. Despeignes, *supra* note 218 (EU Data Privacy restriction not yet imposed on any U.S. company or Web site of consequence but, according to Rep. Tauzin, could lead to effective imposition of a "de-facto privacy standard on the world").

241. Attorney General Ashcroft's proposed curtailment of civil liberties came to fruition on Thursday, October 25, 2001, when the Senate voted, with one lone dissenting vote, to enact the Antiterrorism Bill of 2001. The President signed the bill into law on October 26, 2001. The Senate quickly expanded governmental surveillance powers of the citizenry, and Attorney General of the U.S. Ashcroft requested more wiretapping legislation immediately. John Schwartz, *In Investigation, Internet Offers Clues and Static*, N.Y. TIMES, Sept. 26, 2001, at H-1 (quoting Ronald K. Noble, the secretary general of Interpol: "The big difference between an investigation now and the one after the Oklahoma City bombing is the widespread availability of the Internet"). In response to General Ashcroft's requests of Congress, the public-interest law community, particularly the ACLU, released a statement on Thursday, September 20, 2001, in Washington, D.C.: *In Defense of Freedom at a Time of Crisis, at* http://www.aclu.org/congress/1092001b.htm (last visited October 2, 2001).

242. We would regret a U.S. retrenchment regarding business intrusions into personal data and beg for sharply circumscribed governmental intrusions, with automatic sunset periods, just as we would find the government's racial profiling less efficient than certain other measures such as checking nations of origin on passports and suspicious airline routings.

reading, than the First Amendment right to pay monies to political candidates.

In *Lorillard Tobacco v. Reilly*,[243] the Court held 5-to-4 that local (Boston) and state regulation of tobacco advertising is preempted, concerning cigarette advertisements, by the Federal Cigarette Labeling and Advertising Act of 1965. The federal act specifically states that "no requirement or prohibition based on smoking and health shall be imposed under state law with respect to the advertising or promotion of any cigarette" packaging of smokeless tobacco and cigars in compliance with the health-warning requirements of the federal statute.[244] The usual four dissentients, Justices Stevens, Ginsburg, Breyer and Souter, would say that Congress did not intend the 1965 Act fully to preempt state and local regulation of cigarette advertising but merely "a narrow set of content regulations." "Noble ends do not save a speech-restricting statute whose means are poorly tailored," said Justice Stevens. The four would have remanded the case to allow state regulators to prove that tobacco manufacturers had alternative "sufficient" means of communication of their advertising message.

These fees were assessed under a federal Department of Agriculture program approved in 1990 that authorized a one-penny per pound fee on mushroom producers. Here, Justices Stevens and Souter voted for the free-speech claim. Earlier, in *Glickman v. Wileman Bros.*,[245] the Court held against the free-speech claim of growers of peaches, plums, and nectarines when the federal agricultural program at issue covered marketing orders and advertisements, not merely advertisements. In *Glickman*, Justices Stevens and Souter voted against the "compelled speech" twice on the commercial-free-speech claim. Still in the same Court term, in *Federal Election Commission v. Colorado Republican Party*,[246] the Court upheld federal spending limits imposed on political advertisements made by state and national political parties as against the parties' claimed First Amendment free-speech rights. *FEC v. Colorado Republican Party* is in line with post-Watergate Era precedent, beginning with *Buckley v. Valeo*,[247] the seminal case upholding contribution limits imposed on

243. Lorillard Tobacco Co. v. Reilly, 533 U.S. 525 (2001).

244. Linda Greenhouse, *The Supreme Court: Supreme Court Roundup; Justices Rein in Local Regulation of Tobacco Ads*, N.Y. TIMES, June 29, 2001, at A-1.

245. *Compare* Glickman v. Wileman Bros., 521 U.S. 457 (1997) and United States v. United Foods, Inc., 533 U.S. 405 (2001) on business' claim to be free from making "compelled speech."

246. Federal Election Comm. v. Colorado Republican Fed. Campaign Comm., 533 U.S. 431 (2001).

247. Buckley v. Valeo, 424 U.S. 1 (1976).

political spending. Still again, one must compare the earlier case of *Colorado Republicans v. Federal Election Commission*,[248] which held unconstitutional the federal limits imposed on political parties' "independent expenditures."

Perhaps it is a bit misleading even to use the phrase "mushrooms jurisprudence" to conclude that the current Supreme Court Free Speech analysis holds stronger the First Amendment right to advertise cigarettes and mushrooms than it holds the First Amendment right to pay monies to political candidates. It is, though, in the clear national need to limit the influence of Big Money spending in politics. The Court's rationale supports our thesis; just as the High Court is clearly adopting a policy sympathetic to the national need to limit spending [by influence-peddlers] in political campaigns, the Court should recognize the nation's need to weigh personal data-privacy rights more heavily in the balance than an alleged First Amendment right of commercial interests to collect and disseminate personal data without consent of the data subject.

The right of commercial free speech is not sacred. To quote Professor Tamara Piety:

> The 'sacred' right of free speech is where property owners today seek to protect the right to manipulate us and distort our values to serve their own ends. These are not necessarily society's ends. But it should be remembered that just as the Realists' insights revealed that the existing distribution was not 'natural' in the sense that it was constituted other than by governmental decisions, so too speech. It is worth considering whether the current architecture of the first amendment with respect to commercial speech is one we can afford to live with or whether we may not be imperiling our well being by complacency.[249]

Justice Scalia surprised many Court watchers by finding police use against a private home of thermal imaging radiography, which could detect the growing of marijuana under artificial lights, to be an unconstitutional search and seizure in violation of the Fourth Amendment's grant of privacy from governmental intrusion.[250] His opinion is fundamentally a defense of personal privacy which, it is hoped, bodes well for the personal-data privacy issue. He wrote, "At the very core of the Fourth Amendment stands the right of a man [or woman] to retreat into his [or her] home and

248. Colorado Republicans v. Federal Election Comm., 518 U.S. 604 (1996).

249. Piety, *supra* note 46, at 450.

250. Kyllo v. United States, 533 U.S. 27 (2001) (holding unconstitutional as against the Fourth Amendment the police use of thermal imaging heat-detectors aimed at private homes to detect marijuana-growing lights inside).

there be free." Furthermore, he adjudged, "Where, as here, the government uses a device that is not in general use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a search and is presumptively unreasonable without a warrant."[251]

For the government to point thermal scanners at a home legally, then, the police must first obtain a good search warrant. The same "bright line" sanctity should be carved for the right of a person to expect privacy from business' intrusion for his or her personal data, *simpliciter*. This is true if not from limited *governmental* surveillance in cases of pressing national security needs, then at least from unwarranted and unconsented-to *business* intrusion by computer devices which would, in the Supreme Court's own language, "previously have been unknowable without physical intrusion." Surely the right of informational privacy, to prevent thermal imaging of one's own personal data, as it were, takes primacy of consideration over some poorly-defined, derivative right of "commercial speech" which is economically motivated.

C. *Constitutional Amendment*

The Supreme Court has been very clear that, short of constitutional amendment, only it can delimit the state's power to regulate free speech, including presumably commercial free speech. But regulate it the legislature can. Yet, given the potential intrusiveness of the Internet to personal privacy, it is not enough for the government merely to regulate "false or deceptive" commercial speech.[252]

The U.S. Supreme Court's recent interpretation of "commercial speech" in the *Bigelow* and *Central Hudson* line of cases is an unfortunate, late-twentieth-century, judicial gloss on the First Amendment to the U.S. Constitution. Commercial Speech is a barely-born doctrine that should be reversed, in the public interest. Now, twenty-six years after *Bigelow*'s announcement of the new Doctrine of Commercial Speech, in the face of deleterious effects on U.S. society from "commercial speech,[253] it is time to re-think the so-called freedom of *commercial* speech. This is *a fortiorari* true if the judicially created "right" embraces the right of business to intrude into the informational privacy of individuals.

The *Central Hudson* Court's definition of "commercial speech" reveals flawed logic. For "commercial speech" turns out to be the upside-

---

251. *Id.* at 31.

252. Federal Trade Commission Act, 15 U.S.C.A. § 41 (1914); *see also supra* note 11 and accompanying text.

253. JHALLY, *supra* note 49, SCHUDSON, *supra* note 49, and LASN, *supra* note 49.

down form of *non*commercial speech. While the government can regulate the "truth" of commercial speech, generally the government cannot regulate the truth of *non*commercial free speech, except through tort law. And even the body of U.S. tort law does not allow prior restraint of the free-speech right.[254]

Instead of merely allowing regulation of "false or deceptive" commercial speech, the High Court should frankly allow governmental regulation of "truthful" commercial speech posing harmful societal consequences; and one clear way to measure the harm to society is to consider whether the "truthful" commercial speech would impinge upon the right of personal privacy.[255]

Aware of the dangers to personal privacy posed by data collection from the Internet, whether the data collected are characterized as "true" or "false" commercial speech, the Supreme Court should uphold as constitutional under the First Amendment (and the Fifth Amendment Takings Clause) an omnibus data-privacy statute.[256] Such a statute should exhibit the nature of the requirements which the EU's Data Privacy Directive imposes on the 15-member states of the EU. It would be wrong – and ultimately harmful to business as consumer confidence in the privacy of their engaging in Internet transactions dips ever lower – for the Court to allow further perversion of the idea of "commercial speech" which was designed to protect consumers. Too obvious for all to see readily, evidently, is the correct response to businesses which would identify their interests as coextensive with the interests with consumers: If this argument made by business were so, one could assume that the consumer could curtail business' incursions into personal privacy.

---

254. Tort law offers a few exceptions, such as providing a cause of action for defamation, but does not authorize prior judicial restraint of noncommercial speech. YASSER ET AL., *supra* note 116, at 767-69.

255. The U.S. Supreme Court, after all, has allowed an even "fuzzier" definition of "obscenity" which latter term implicates the First Amendment freedom of non-commercial speech: "We know it when we see it." Jacobellis v. Ohio, 378 U.S. 184,197 (1964) (Stewart, J., concurring).

256. Professor Fred H. Cate of Indiana University School of Law, Bloomington, and Senior Counsel for Information Law, Ice Miller Donadio & Ryan, disagrees. He reads the Supreme Court's decision in *Liquormart, Inc. v. Rhode Island*, 517 U.S. 484, 509 (1996) as prelude for a judicial decision that the First Amendment would prohibit a ban on use of personal data in the nature of the ban mandated by the 1995 EU Data Privacy Directive. In *Liquormart*, the Court says the Court made a flawed analysis of the First Amendment in *Posados de Puerto Rico Assoc. v. Tourism Co. of Puerto Rico,* 478 U.S. 328 (1986) when the Court allowed its examination of the First Amendment to defer to the legislature. Cate, *supra* note 35, at 232.

This review of the pertinent U.S. case law has shown that the Court has strayed far from its theoretical foundations laid in *Bigelow*. In 1975 the Court rendered *Bigelow* solely for the purpose of making sure that consumers received information correctly. Indeed the rationale could be stated as the right of listeners of commercial speech truthfully to be informed. Even under *Bigelow*, consumers in the information age should have primacy of judicial consideration for their personally identified or identifiable data over commercial-free-speech rights.

Instead of merely allowing regulation of "false or deceptive" commercial speech, the High Court, aware of the dangers to personal privacy posed by data collection from the Internet, whether the data collected are characterized as "true" or "false" commercial speech, should uphold as constitutional under the First Amendment (and the Fifth Amendment Takings Clause) an omnibus data-privacy statute.[257]

As mentioned, the United States Supreme Court's *Hill v. Colorado*[258] decision can be read as presaging the Court's inclination to uphold a comprehensive data-privacy statute enacted by Congress. And we take heart from Chief Justice Rehnquist's dissenting opinion in *Bartnicki v. Vopper*, in which Justices Scalia and Thomas joined. In their cellular telephone conversation, Chief Justice Rehnquist complains:

> Bartnicki and Kane had no intention of contributing to a public 'debate' at all, and it is perverse to hold that another's unlawful interception and knowing disclosure of their conversation is 'speech worthy of constitutional protection.' [citations omitted] Surely 'the interest in individual privacy,' . . . at its narrowest must embrace the right to be free from surreptitious eavesdropping on, and involuntary broadcast of, our cellular telephone conversations.[259]

If the Supreme Court cannot in conscience, though, find legal support for an omnibus statute under its traditional tests, it should adopt outright the European Principle of Proportionality to save a statute. Unfortunately, the fact that Senator Hollings' bill[260] tracking the FTC's 2000 Report remains long stalled in Congress does not inspire confidence in the legislative route.

---

257. *See supra* note 256 and accompanying text.

258. Hill v. Colorado, 530 U.S. 703 (2000).

259. Bartnicki v. Vopper, 532 U.S. 514, 554-56 (2001) (dissent by Rehnquist, C.J.). *See also* Martin H. Belsky, *Privacy: The Rehnquist Court's Unmentionable "Right,"* 36 TULSA L. J. 43 (2000).

260. The Consumer Privacy Protection Act of 2000, S. 2606 (pending bill of Senator Hollings, recommending data-privacy legislation).

What if, nevertheless, an international treaty fails or an effective privacy statute cannot be enacted by Congress or, once enacted, cannot be saved from a judicial finding of unconstitutionality? There may then be no recourse for those genuinely concerned for the integrity of individual privacy, as a keystone for modern society, but to seek amendment to the U.S. Constitution.

The United States Constitution allows two methods for amendment. Article V of the United States Constitution states:

> The Congress, whenever two thirds of both Houses shall deem it necessary, shall propose Amendments to this Constitution, or, on the Application of the Legislatures of two thirds of the several States, shall call a Convention for proposing Amendments, which, in either Case, shall be valid to all Intents and Purposes, as part of this Constitution, when ratified by the Legislatures of three fourths of the several States, or by Conventions in three fourths thereof, as the one of the other Mode of Ratification which may be proposed by the Congress; Provided that no Amendment which maybe made prior to the Year One thousand eight hundred and eight shall in any Manner affect the first and fourth Clauses in the Ninth Section of the first Article; and that no State, without its Consent, shall be deprived of its equal Suffrage in the Senate.[261]

It was the state legislatures after the Revolutionary War against England that abjured the Articles of Confederation and met *ultra vires* to write the Constitution. Fear of runaway state legislatures has restricted the means of constitutional amendment to only one of the two methods allowed by the Constitution.

The privacy watchdog, Center for Democracy & Technology, not to be dismissed as a hapless Cassandra betrayed by Apollo, has prophesied:

> Direct marketing, personalized and targeted with an unprecedented precision, may benefit individual consumers and the on-line market on the whole. However great the potential benefits of on-line tracking, they remain incomparable to the grave implications of Internet users' loss of privacy.[262]

---

261. U.S. CONST. art. V.

262. "The Internet is a microcosm of the debate over privacy and technology's impact on the collection of personal information. Internet use generates detailed information about individuals—revealing where they "go" on the Net (via *URLs*), whom they associate with (via list-servs, chat rooms and news groups), and how they engage in political activities and social behavior. Various tracking tools can mine and manipulate your on-line data trail (or "clickstream") to build a detailed database of personal information without your

We cannot improve upon this warning. Perhaps, as Professor Balkin has predicted, the issue of free speech will be to twenty-first century U.S. law what *Lochner*[263] was to twentieth-century jurisprudence.

If Directive 95/46/EC of the European Union has forced the U.S. government to consider the invasiveness of currently accepted business practice and to enact ameliorative law, then American society, in particular the consumer who alone pitted against business' short-term interests carries little political weight, owes much to the European privacy impetus. It would benefit global society to adopt the philosophy of the directive as the new *ius gentium* for data-privacy law.

True, reasonable data-privacy requirements imposed by either constitutional amendment or omnibus national privacy legislation would necessarily require U.S. on-line data gatherers and users to adjust their business models. And, yes, restricting data access would compromise to some degree America's vaunted open society, thereby in the process almost certainly raising the ACLU's First Amendment hackles, as has the Patriot or Anti-Terrorism Bill.

Nevertheless, as between imposing correction costs upon commercial interests, as the 1995 EU Data Privacy Directive (Directive 95/46/EC) does, and allowing untrammeled use of private, personal information, the First Amendment freedom of so-called commercial speech, made for purely economic motives, is decidedly inferior to the right of human privacy which a consumer data subject reasonably expects as a bulwark against serious intrusion. If interest groups with vested interests and the legislative and judicial branches of the U.S. government cannot support an omnibus privacy statute, there may be no recourse for those genuinely concerned for the integrity of individual privacy but to seek amendment to the U.S. Constitution. In any event the personal right to the privacy of one's own personal data should trump the more questionable right to engage in "commercial speech" for which the speaker's motive is purely economic. The U.S. should follow the lead of the EU and embrace the hierarchy of rights enunciated in the EU's 1995 Data Privacy Directive.

---

knowledge or consent." Center for Democracy & Technology, *at* http://www.cdt.org/privacy (last visited Oct. 12, 2001).

263. Lochner v. New York, 198 U.S. 45 (1905). See also BALKIN, *supra* note 125.